

特開2001-175606

(P2001-175606A)

(43)公開日 平成13年6月29日(2001.6.29)

(S1)Int.Cl. <sup>7</sup>	識別記号	F I	レイアウト <sup>8</sup> (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z 5 B 0 8 5
	13/00		3 5 4 Z 5 B 0 8 9
G 1 0 L 11/00		H 0 4 H 1/00	F 5 J 1 0 4
H 0 4 H 1/00		G 1 0 L 9/00	E 9 A 0 0 1
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 A
		審査請求 未請求	請求項の数56 O L (全148頁)

審査請求 未請求 請求項の数56 OL (全148頁)

(21)出願番号 特願平11-361225

(22)出願日 平成11年12月20日(1999.12.20)

(71)出願人 000002185  
ソニー株式会社  
東京都品川区北品川6丁目7番35号

(72)発明者 野中 聡  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(72)発明者 江崎 正  
東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(74)代理人 100094053  
弁理士 佐藤 隆久

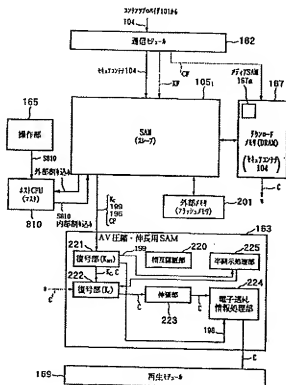
[最終頁に続く](#)

(54) 【発明の名称】 データ処理装置、データ処理機器およびその方法

(57) 【要約】

【課題】 コンテンツデータの提供者の利益を効果的に保護できるデータ処理装置を提供する。

【解決手段】 SAM105<sub>1</sub> は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを格納したセキュアコンテンツリポジトリ104を入力し、権利書データが示す取り扱いに基づいて、コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。SAM105<sub>1</sub> は、ホストCPU810のスレーブとして機能すると共に、ホストCPU810との共有メモリを有している。



**【特許請求の範囲】**

【請求項1】コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置において、

第1のバスと、

前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第1のバスに接続された演算処理回路と、

前記第1のバスに接続された記憶回路と、

第2のバスと、

前記第1のバスと前記第2のバスとの間に介在するインターフェイス回路と、

前記第2のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、

前記第2のバスに接続された外部バスインターフェイス回路とを耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項2】前記インターフェイス回路を第1のインターフェイス回路とした場合に、前記第1のバスは、前記演算処理回路および前記記憶回路に接続された第3のバスと、前記第1のインターフェイス回路に接続された第4のバスとを有し、

前記データ処理装置は、

前記第3のバスと前記第4のバスとの間に介在する第2のインターフェイス回路を前記耐タンパ性の回路モジュール内にさらに有する請求項1に記載のデータ処理装置。

【請求項3】第5のバスと、

記録媒体またはICカードに搭載された認証機能を持つデータ処理回路との間の通信処理を行い、前記第5のバスに接続された第3のインターフェイス回路と、前記第4のバスと前記第5のバスとの間に介在する第4のインターフェイス回路とを前記耐タンパ性の回路モジュール内にさらに有する請求項2に記載のデータ処理装置。

【請求項4】前記暗号処理回路は、

公開鍵暗号回路と、

共通鍵暗号回路とを有する請求項1に記載のデータ処理装置。

【請求項5】前記記憶回路は、当該データ処理装置の秘密鍵データおよび他の装置の公開鍵データを記憶し、前記公開鍵暗号回路は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する前記公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成し、

前記共通鍵暗号回路は、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する請求項4に記載のデータ処理装置。

【請求項6】前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのハッシュ値を生成するハッシュ値生成回路を前記耐タンパ性の回路モジュール内にさらに有し、

前記公開鍵暗号回路は、前記ハッシュ値を用いて、前記署名データの検証および前記署名データの作成を行う請求項5に記載のデータ処理装置。

【請求項7】前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該他の装置との間の相互認証を行うために乱数を生成し、前記第2のバスに接続された乱数生成回路を前記耐タンパ性の回路モジュール内にさらに有する請求項1に記載のデータ処理装置。

【請求項8】前記外部バスインターフェイス回路は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路と接続される請求項1に記載のデータ処理装置。

【請求項9】前記記憶回路に対してのアクセスと、前記外部バスインターフェイスを介した前記外部記憶回路に対してのアクセスとの制御を、前記演算処理回路からの命令に応じて行う記憶回路制御回路とをさらに有する請求項8に記載のデータ処理装置。

【請求項10】前記外部バスインターフェイス回路は、当該データ処理装置が搭載された機器の制御を統括的に行うホスト演算処理装置に接続される請求項1に記載のデータ処理装置。

【請求項11】前記記憶回路および前記外部記憶回路のアドレス空間を管理する記憶管理回路をさらに有する請求項8に記載のデータ処理装置。

【請求項12】前記演算処理回路は、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する請求項1に記載のデータ処理装置。

【請求項13】前記演算処理回路は、前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成し、前記利用制御データに基づいて、前記コンテンツデータの利用を制御する請求項12に記載のデータ処理装置。

【請求項14】前記共通鍵暗号回路は、前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合

に、前記コンテンツ鍵データおよび前記利用制御データを、前記記録媒体に対応したメディア鍵データを用いて暗号化する請求項4に記載のデータ処理装置。

【請求項15】有効期限を持つライセンス鍵データを用いて前記コンテンツ鍵データが暗号化されている場合に、

前記記憶回路は、前記ライセンス鍵データを記憶し、前記データ処理装置は、実時間を生成するリアルタイムクロックをさらに有し、

前記演算処理回路は、リアルタイムクロックが示す実時間に基づいて、有効期限内の前記ライセンス鍵データを前記記憶回路から読み出し、

前記共通鍵暗号回路は、前記読み出されたライセンス鍵データを用いて、前記コンテンツ鍵データを復号する請求項4に記載のデータ処理装置。

【請求項16】前記記憶回路は、ブロック単位でデータの書き込みおよび消去が行われ、

前記演算処理回路によって制御され、前記記憶回路に対してのデータの書き込みおよび消去の許可を前記ブロック単位で管理する書き込みロック制御回路を前記耐タンパ性の回路モジュール内にさらに有する請求項1に記載のデータ処理装置。

【請求項17】コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置において、

第1のバスと、

前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第1のバスに接続された演算処理回路と、

前記第1のバスに接続された記憶回路と、

第2のバスと、

前記第1のバスと前記第2のバスとの間に介在するインターフェイス回路と、

前記第2のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、

前記第2のバスに接続された外部バスインターフェイス回路とを耐タンパ性の回路モジュール内に有し、

前記演算処理回路は、前記外部バスインターフェイス回路を介して外部回路から割り込みを受けると、当該外部回路のスレーブとなつて当該割り込みによって指定された処理を行い、当該処理の結果を前記外部装置に通知するデータ処理装置。

【請求項18】前記演算処理回路は、前記処理の結果を前記外部回路に割り込みを出して通知する請求項17記載のデータ処理装置。

【請求項19】前記外部バスインターフェイスは、前記演算処理回路および前記外部回路との共有メモリを有し、前記演算処理回路は、当該共有メモリに前記処理の結果

を書き込み、当該処理の結果は前記外部回路からのポーリングによって当該外部回路に通知される請求項17に記載のデータ処理装置。

【請求項20】前記外部バスインターフェイスは、前記外部回路から依頼された処理の前記演算処理回路における実行状態を示し、前記演算処理回路によって設定され、前記外部回路によって読まれるフラグを持つ第1のステータスレジスタと、

前記外部回路が前記演算処理回路に処理を依頼したか否かを示し、前記外部回路によって設定され、前記演算処理回路によって読まれるフラグを持つ第2のステータスレジスタと、

前記処理の結果が書き込まれる記憶回路とを有する請求項19に記載のデータ処理装置。

【請求項21】前記記憶回路は、前記割り込みによって指定される処理を記述した割り込みプログラムを記憶し、

前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行して前記処理を行う請求項18に記載のデータ処理装置。

【請求項22】前記記憶回路は、複数の前記割り込みプログラムと、当該割り込みプログラムを実行する際に読み出される複数のサブルーチンとを記憶し、前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行する際に、前記記憶回路から必要に応じて前記サブルーチンを読み出して実行する請求項21に記載のデータ処理装置。

【請求項23】所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなつて所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置とを有するデータ処理機器において、

前記データ処理装置は、権利書データが示す取り扱いに基づいて、コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理機器。

【請求項24】前記演算処理装置は、前記割り込みタイプを示す割り込みを受けると、当該割り込みタイプに対応した割り込みルーチンを実行して割り込みを前記データ処理装置に出し、

前記データ処理装置は、前記演算処理装置から受けた前記割り込みによって指定された処理に対応する割り込みルーチンを実行する請求項23に記載のデータ処理機器。

【請求項25】前記データ処理装置は、前記処理の結果

を前記演算処理装置に割り込みを出して通知する請求項23に記載のデータ処理機器。

【請求項26】前記データ処理装置は、当該データ処理装置および前記演算処理装置がアクセス可能な共有メモリを有し、

前記演算処理装置は、ボーリングによって、前記共有メモリにアクセスを行って前記処理の結果を得る請求項23に記載のデータ処理機器。

【請求項27】前記データ処理装置は、前記演算処理装置から前記割り込みによって依頼された処理の実行状態を示し、前記演算処理装置によって読まれるフラグを持つ第1のステータスレジスタと、前記演算処理装置が当該データ処理装置に前記割り込みによって処理を依頼したか否かを示し、前記演算処理装置によって設定されるフラグを持つ第2のステータスレジスタと、

前記処理の結果が書き込まれる前記共有メモリとを有する請求項26に記載のデータ処理機器。

【請求項28】前記演算処理装置と、前記データ処理装置とを接続するバスをさらに有する請求項23に記載のデータ処理機器。

【請求項29】前記データ処理装置は、初期プログラムまたは前記割り込みルーチンの実行を終了した後に、低消費電力状態になる請求項24に記載のデータ処理機器。

【請求項30】前記データ処理装置は、前記演算処理装置から受けた前記割り込みに基づいて、前記コンテンツデータの購入形態または利用形態の決定処理、前記コンテンツデータの再生処理および権威機関からのデータのダウンロード処理のうち少なくとも一の処理に対応する前記割り込みルーチンを実行する請求項24に記載のデータ処理機器。

【請求項31】前記演算処理装置は、所定のユーザプログラムを実行する請求項23に記載のデータ処理機器。

【請求項32】データ提供装置が提供したコンテンツデータをデータ配給装置から受け、管理装置によって管理されるデータ処理機器において、

前記データ提供装置が提供した、コンテンツ鍵データを用いた暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、前記データ配給装置から受信し、共有鍵データを用いて前記受信したモジュールを復号し、前記データ配給装置による前記モジュールの配給サービスに対しての課金処理を行う第1の処理モジュールと、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行

い、当該処理の結果を前記演算処理装置に通知するデータ処理装置であって、前記受信したモジュールに格納された権利書データが示す取り扱いに基づいて、前記受信したモジュールに格納されたコンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置とを有するデータ処理機器。

【請求項33】所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第1のデータ処理装置と、前記演算処理装置あるいは前記第1のデータ処理装置から割り込みを受けて、マスタである前記演算処理装置あるいは前記第1のデータ処理装置のスレーブとなって、前記第1のデータ処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第2のデータ処理装置とを有するデータ処理機器。

【請求項34】前記演算処理装置、前記第1のデータ処理装置および前記第2のデータ処理装置を接続するバスをさらに有する請求項33に記載のデータ処理機器。

【請求項35】所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第1のデータ処理装置と、前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第2のデータ処理装置とを有するデータ処理機器。

【請求項36】前記第2のデータ処理装置は、前記記録媒体に対応したメディア鍵データを用いて、前記コンテンツデータの復号および暗号化を行う請求項35に記載のデータ処理機器。

【請求項37】前記第2のデータ処理装置は、前記記録媒体が相互認証機能を持つ処理回路を搭載している場合に、前記処理回路との間で相互認証を行う請求項35に記載のデータ処理機器。



【請求項38】所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第1のデータ処理装置と、前記演算処理装置が出した割り込みに応じて、マスクである前記演算処理装置のスレブとなつて、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第2のデータ処理装置とを有するデータ処理機器。

【請求項39】前記第1のデータ処理装置が前記記録媒体から読み出した前記コンテンツデータを一時的に記憶し、当該記憶したコンテンツデータを前記第2のデータ処理装置に出力する記憶回路をさらに有する請求項38に記載のデータ処理機器。

【請求項40】前記記憶回路は、耐振動用記憶回路の記憶領域の一部をその記憶領域とする請求項39に記載のデータ処理機器。

【請求項41】前記演算処理装置から割り込みを受けて、マスクである前記演算処理装置のスレブとなつて、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第3のデータ処理装置をさらに有する請求項38に記載のデータ処理機器。

【請求項42】演算処理装置およびデータ処理装置を用いたデータ処理方法において、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記データ処理装置は、前記演算処理装置から割り込みを受けて、マスクである前記演算処理装置のスレブとなつて、耐タンパ性の回路モジュール内で、権利書データが示す取り扱いに基づいて、当該権利書データに対応したコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定の結果を示す履歴データを生成し、前記コンテンツ鍵データを復号するデータ処理方法。

【請求項43】前記演算処理装置は、前記割り込みタイプを示す割り込みを受けると、当該割り込みタイプに対応した割り込みルーチンを実行して割り込みを前記データ処理装置に出し、前記データ処理装置は、前記演算処理装置から受けた前記割り込みによって指定された処理に対応する割り込みルーチンを実行する請求項42に記載のデータ処理方法。

【請求項44】前記データ処理装置は、前記処理の結果を前記演算処理装置に割り込みを出して通知する請求項42に記載のデータ処理機器。

【請求項45】前記データ処理装置は、当該データ処理

装置および前記演算処理装置がアクセス可能な共有メモリを有し、

前記演算処理装置は、ポーリングによって、前記共有メモリにアクセスを行つて前記処理の結果を得る請求項42に記載のデータ処理方法。

【請求項46】前記データ処理装置は、前記演算処理装置から前記割り込みによって依頼された処理の実行状態を示す第1のステータスレジスタのフラグを設定し、前記演算処理装置は、前記第1のステータスレジスタのフラグから、前記データ処理装置の処理の実行状態を把握し、

前記演算処理装置は、前記データ処理装置に前記割り込みによって処理を依頼したことを示す第2のステータスレジスタのフラグに設定し、

前記データ処理装置は、前記第2のステータスレジスタのフラグから、前記演算処理装置が前記割り込みによって処理を依頼したか否かを把握する請求項45に記載のデータ処理方法。

【請求項47】前記データ処理装置は、初期プログラムまたは前記割り込みルーチンの実行を終了した後に、低消費電力状態になる請求項42に記載のデータ処理方法。

【請求項48】前記データ処理装置は、前記演算処理装置から受けた前記割り込みに基づいて、前記コンテンツデータの購入形態または利用形態の決定処理、前記コンテンツデータの再生処理および権威機関からのデータのダウンロード処理のうち少なくとも一の処理に対応する前記割り込みルーチンを実行する請求項42に記載のデータ処理方法。

【請求項49】前記演算処理装置は、所定のユーザプログラムを実行する請求項42に記載のデータ処理方法。

【請求項50】演算処理装置、第1のデータ処理装置および第2のデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記第1のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスクである前記演算処理装置のスレブとなつて、耐タンパ性のモジュール内で、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、

前記第2のデータ処理装置は、前記演算処理装置あるいは前記第1のデータ処理装置から割り込みを受けて、マスクである前記演算処理装置あるいは前記第1のデータ処理装置のスレブとなつて、耐タンパ性のモジュール内で、前記第1のデータ処理装置から相互認証を行つて得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行うデータ処理方法。

【請求項51】演算処理装置、第1のデータ処理装置および第2のデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記第1のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなつて、耐タンパ性のモジュール内で、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、

前記第2のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行うデータ処理方法。

【請求項52】前記第2のデータ処理装置は、前記記録媒体に対応したメディア鍵データを用いて、前記コンテンツデータの復号および暗号化を行う請求項51に記載のデータ処理方法。

【請求項53】前記第2のデータ処理装置は、前記記録媒体が相互認証機能を持つ処理回路を搭載している場合に、前記処理回路との間で相互認証を行う請求項51に記載のデータ処理方法。

【請求項54】演算処理装置、第1のデータ処理装置および第2のデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記第1のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行い、

前記第2のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなつて、耐タンパ性のモジュール内で、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行うデータ処理方法。

【請求項55】前記第1のデータ処理装置が前記記録媒体から読み出した前記コンテンツデータを記憶回路に一時的に記憶し、当該記憶回路から読み出したコンテンツデータを前記第2のデータ処理装置に出力する請求項54に記載のデータ処理方法。

【請求項56】前記記憶回路として、耐振動用記憶回路の記憶領域の一部をその記憶領域を用いる請求項55に記載のデータ処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、提供されたコンテンツデータに関連する処理を行うデータ処理装置、データ処理機器およびその方法に関する。

【0002】

【従来の技術】暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に供給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。このようなデータ提供システムの一つに、音楽データを配信する従来のEMD(Electronic Music Distribution: 電子音楽配信)システムがある。

【0003】図106は、従来のEMDシステム700の構成図である。図106に示すEMDシステム700では、コンテンツプロバイダ701a、701bが、サービスプロバイダ710に対し、コンテンツデータ704a、704b、704cと、著作権情報705a、705b、705cとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報705a、705b、705cには、例えば、SCMS(Serial Copy Management System)情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ710の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【0004】サービスプロバイダ710は、受信したコンテンツデータ704a、704b、704cと、著作権情報705a、705b、705cとをセッション鍵データを用いて復号する。そして、サービスプロバイダ710は、復号したあるいはオフラインで受け取ったコンテンツデータ704a、704b、704cと、著作権情報705a、705b、705cを埋め込んで、コンテンツデータ707a、707b、707cを生成する。このとき、サービスプロバイダ710は、例えば、著作権情報705a、705b、705cのうち電子透かし情報をコンテンツデータ704a、704b、704cに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにSCMS情報を埋め込む。さらに、サービスプロバイダ710は、コンテンツデータ707a、707b、707cを、鍵データベース706から読み出したコンテンツ鍵データKca、Kcb、Kccを用いてそれぞれ暗号化する。その後、サービスプロバイダ710は、暗号化されたコンテンツデータ707a、707b、707cを格納したセキュアコンテナ722を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置709に存在するCA(Conditional Access)モジュール711に送信する。

【0005】CAモジュール711は、セキュアコンテナ722をセッション鍵データを用いて復号する。また、CAモジュール711は、電子決済やCAなどの課

金機能を用いて、サービスプロバイダ710の鍵データベース706からコンテンツ鍵データKca, Kcb, Kccを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置709において、コンテンツデータ707a, 707b, 707cを、それぞれコンテンツ鍵データKca, Kcb, Kccを用いて復号することが可能になる。このとき、CAモジュール711は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報721を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ710の権利処理モジュール720に送信する。この場合に、CAモジュール711は、サービスプロバイダ710が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティ確保とを行う。

【0006】サービスプロバイダ710は、CAモジュール711から課金情報721を受信すると、サービスプロバイダ710とコンテンツプロバイダ701a, 701b, 701cとの間で利益配分を行う。このとき、サービスプロバイダ710から、コンテンツプロバイダ701a, 701b, 701cへの利益配分は、例えば、JASRAC(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会)を介して行われる。また、JASRACによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【0007】また、端末装置709では、コンテンツ鍵データKca, Kcb, Kccを用いて復号したコンテンツデータ707a, 707b, 707cを、RAM型の記録媒体723などに記録する際に、著作権情報705a, 705b, 705cのSCMSビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ707a, 707b, 707cに埋め込まれたSCMSビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【0008】

【発明が解決しようとする課題】ところで、SCMSは、コンテンツデータを例えば2世代以上のわたって複製することを禁止するものであり、1世代の複製は無制限に行うことができ、著作権者の保護として不十分であるという問題がある。

【0009】また、上述したEMDシステム700では、サービスプロバイダ710が暗号化されていないコンテンツデータを技術的に自由に扱えるため、コンテンツプロバイダ701の関係者はサービスプロバイダ710の行為等を監視する必要があるが、当該監視の負担が大きいと共に、コンテンツプロバイダ701の利益が不当に損なわれる可能性が高いという問題がある。また、上

述したEMDシステム700では、ユーザの端末装置709がサービスプロバイダ710から配給を受けたコンテンツデータをオースラリングして他の端末装置などに再配給する行為を規制することが困難であり、コンテンツプロバイダ701の利益が不当に損なわれるという問題がある。

【0010】本発明は上述した従来技術の問題点に鑑みてなされ、コンテンツプロバイダの権利者（関係者）の利益を適切に保護するシステムおよび方法に適用可能なデータ処理装置、データ処理機器およびその方法を提供することを目的とする。また、本発明は、コンテンツプロバイダの権利者の利益を保護するための監査の負担を軽減するシステムおよび方法に適用可能なデータ処理装置、データ処理機器およびその方法を提供することを目的とする。

【0011】

【課題を解決するための手段】上述した目的を達成するために、本発明の第1の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置であって、第1のバスと、前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第1のバスに接続された演算処理回路と、前記第1のバスに接続された記憶回路と、第2のバスと、前記第1のバスと前記第2のバスとの間に介在するインターフェイス回路と、

前記第2のバスに接続され、前記コンテンツデータの復号を行う暗号処理回路と、前記第2のバスに接続された外部バスインターフェイス回路とを耐タンパ性の回路モジュール内に有する。

【0012】本発明の第1の観点のデータ処理装置では、例えば、コンテンツデータおよびそれに対応したコンテンツ鍵データおよび権利書データが配給と、暗号化されたコンテンツ鍵データを復号するライセンス鍵データが配給される。ここで、ライセンス鍵データは、例えば、前記記憶回路に記憶される。そして、例えば、外部バスインターフェイス回路を介して、外部の演算処理装置から権利処理などを行う指示が出されると、前記演算処理回路において、権利書データに基づいたコンテンツデータの権利処理が行われる。その後、暗号処理回路において、記憶回路から読み出したライセンス鍵データを用いて、コンテンツ鍵データの復号が行われる。そして、第1の観点のデータ処理装置は、他の復号装置との間で互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記復号したコンテンツ鍵データおよびコンテンツデータを暗号化し、当該暗号化したコンテンツ鍵データおよびコンテンツデータを前記他の復号装置に送る。

【0013】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記インターフェイス回路を第1の

インターフェイス回路とした場合に、前記第1のバスは、前記演算処理回路および前記記憶回路に接続された第3のバスと、前記第1のインターフェイス回路に接続された第4のバスとを有し、前記データ処理装置は、前記第3のバスと前記第4のバスとの間に介在する第2のインターフェイス回路を前記耐タンパ性の回路モジュール内にさらに有する。

【0014】また、本発明の第1の観点のデータ処理装置は、好ましくは、第5のバスと、記録媒体またはICカードに搭載された認証機能を持つデータ処理回路との間の通信処理を行い、前記第5のバスに接続された第3のインターフェイス回路と、前記第4のバスと前記第5のバスとの間に介在する第4のインターフェイス回路とを前記耐タンパ性の回路モジュール内にさらに有する。

【0015】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記暗号処理回路は、公開鍵暗号回路と、共通鍵暗号回路とを有する。

【0016】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記記憶回路は、当該データ処理装置の秘密鍵データおよび他の装置の公開鍵データを記憶し、前記公開鍵暗号回路は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データに対応する前記公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成し、前記共通鍵暗号回路は、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する。

【0017】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのハッシュ値を生成するハッシュ値生成回路を前記耐タンパ性の回路モジュール内にさらに有し、前記公開鍵暗号回路は、前記ハッシュ値を用いて、前記署名データの検証および前記署名データの作成を行う。

【0018】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該他の装置との間の相互認証を行うために乱数を生成し、前記第2のバスに接続された乱数生成回路を前記耐タンパ性の回路モジュール内にさらに有する。

【0019】また、本発明の第1の観点のデータ処理装

置は、好ましくは、前記外部バスインターフェイス回路は、当該データ処理装置が搭載された機器の制御を統括的に行うホスト演算処理装置に接続される。

【0020】また、本発明の第1の観点のデータ処理装置は、前記演算処理回路は、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する。

【0021】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記演算処理回路は、前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成し、前記利用制御データに基づいて、前記コンテンツデータの利用を制御する。

【0022】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記共通鍵暗号回路は、前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記記録媒体に対応したメディア鍵データとを用いて暗号化する。

【0023】また、本発明の第1の観点のデータ処理装置は、好ましくは、有効期限を持つライセンス鍵データを用いて前記コンテンツ鍵データが暗号化されている場合に、前記記憶回路は、前記ライセンス鍵データを記憶し、前記データ処理装置は、実時間を生成するリアルタイムクロックをさらに有し、前記演算処理回路は、リアルタイムクロックが示す実時間に基づいて、有効期限内の前記ライセンス鍵データを前記記憶回路から読み出し、前記共通鍵暗号回路は、前記読み出されたライセンス鍵データを用いて、前記コンテンツ鍵データを復号する。

【0024】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記記憶回路は、ブロック単位でデータの書き込みおよび消去が行われ、前記演算処理回路によって制御され、前記記憶回路に対してのデータの書き込みおよび消去の許可を前記ブロック単位で管理する書き込みロック制御回路を前記耐タンパ性の回路モジュール内にさらに有する。

【0025】また、本発明の第2の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置であって、第1のバスと、前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第1のバスに接続された演算処理回路と、前記第1のバスと前記第2のバスとの間に介在するインターフェイス回路と、前記第2のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、前記第2のバスに接続された外部バスインターフェイス回路と耐タンパ性の回路モジュール内に有し、前記演算処理回路は、

前記外部バスインターフェイス回路を介して外部回路から割り込みを受けると、当該外部回路のスレーブとなって当該割り込みによって指定された処理を行い、当該処理の結果を前記外部装置に通知する。

【0026】また、本発明の第2の観点のデータ処理装置は、好ましくは、前記演算処理回路は、前記処理の結果を前記外部回路に割り込みを出して通知する。

【0027】また、本発明の第2の観点のデータ処理装置は、好ましくは、前記外部バスインターフェイスは、前記演算処理回路および前記外部回路との共有メモリを有し、前記演算処理回路は、当該共有メモリに前記処理の結果を書き込み、当該処理の結果は前記外部回路からのポーリングによって当該外部回路に通知される。

【0028】また、本発明の第2の観点のデータ処理装置は、好ましくは、前記外部バスインターフェイスは、前記外部回路から依頼された処理の前記演算処理回路における実行状態を示し、前記演算処理回路によって設定され、前記外部回路によって読まれるフラグを持つ第1のステータスレジスタと、前記外部回路が前記演算処理回路に処理を依頼したか否かを示し、前記外部回路によって設定され、前記演算処理回路によって読まれるフラグを持つ第2のステータスレジスタと、前記処理の結果が書き込まれる記憶回路とを有する。

【0029】また、本発明の第2の観点のデータ処理装置は、好ましくは、前記記憶回路は、前記割り込みによって指定される処理を記述した割り込みプログラムを記憶し、前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行して前記処理を行う。

【0030】また、本発明の第2の観点のデータ処理装置は、好ましくは、前記記憶回路は、複数の前記割り込みプログラムと、当該割り込みプログラムを実行する際に読み出される複数のサブルーチンとを記憶し、前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行する際に、前記記憶回路から必要に応じて前記サブルーチンを読み出して実行する。

【0031】また、本発明の第1の観点のデータ処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置とを有するデータ処理装置であって、前記データ処理装置は、権利書データが示す取り扱いに基づいて、コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【0032】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記演算処理装置は、前記割り込みタイプを示す割り込みを受けると、当該割り込みタイプ

に対応した割り込みルーチンを実行して割り込みを前記データ処理装置に出し、前記データ処理装置は、前記演算処理装置から受けた前記割り込みによって指定された処理に対応する割り込みルーチンを実行する。

【0033】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記データ処理装置は、前記処理の結果を前記演算処理装置に割り込みを出して通知する。

【0034】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記データ処理装置は、当該データ処理装置および前記演算処理装置がアクセス可能な共有メモリを有し、前記演算処理装置は、ポーリングによって、前記共有メモリにアクセスを行って前記処理の結果を得る。

【0035】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記データ処理装置は、前記演算処理装置から前記割り込みによって依頼された処理の実行状態を示し、前記演算処理装置によって読まれるフラグを持つ第1のステータスレジスタと、前記演算処理装置が当該データ処理装置に前記割り込みによって処理を依頼したか否かを示し、前記演算処理装置によって設定されるフラグを持つ第2のステータスレジスタと、前記処理の結果が書き込まれる前記共有メモリとを有する。

【0036】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記データ処理装置は、初期プログラムまたは前記割り込みルーチンの実行を終了した後、に低消費電力状態になる。

【0037】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記データ処理装置は、前記演算処理装置から受けた前記割り込みに基づいて、前記コンテンツデータの購入形態または利用形態の決定処理、前記コンテンツデータの再生処理および権威機関からのデータのダウンロード処理のうち少なくとも一の処理に対応する前記割り込みルーチンを実行する。

【0038】また、本発明の第1の観点のデータ処理装置は、好ましくは、前記演算処理装置は、所定のユーザプログラムを実行する。

【0039】また、本発明の第2の観点のデータ処理装置は、データ提供装置が提供したコンテンツデータをデータ供給装置から受け、管理装置によって管理されるデータ処理装置であって、前記データ提供装置が提供した、コンテンツ暗号データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ供給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、前記データ供給装置から受信し、共有鍵データを用いて前記受信したモジュールを復号し、前記データ供給装置による前記モジュールの供給サービスに対しての課金処理を行う第1の処理モジュールと、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記

演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置であって、前記受信したモジュールに格納された権利書データが示す取り扱いに基づいて、前記受信したモジュールに格納されたコンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置とを有する。

【0040】また、本発明の第3の観点のデータ処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第1のデータ処理装置と、前記演算処理装置あるいは前記第1のデータ処理装置から割り込みを受けて、マスタである前記演算処理装置あるいは前記第1のデータ処理装置のスレーブとなって、前記第1のデータ処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第2のデータ処理装置とを有する。

【0041】また、本発明の第4の観点のデータ処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第1のデータ処理装置と、前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第2のデータ処理装置とを有する。

【0042】また、本発明の第4の観点のデータ処理装置は、好ましくは、前記第2のデータ処理装置は、前記記録媒体に対応したメディア鍵データを用いて、前記コンテンツデータの復号および暗号化を行う。

【0043】また、本発明の第4の観点のデータ処理装置は、好ましくは、前記第2のデータ処理装置は、前記記録媒体が相互認証機能を持つ処理回路を搭載している場合に、前記処理回路との間で相互認証を行う。

【0044】また、本発明の第5の観点のデータ処理装置は、所定のプログラムを実行し、所定の条件で割り込

みを出す演算処理装置と、前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第1のデータ処理装置と、前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第2のデータ処理装置とを有する。

【0045】また、本発明の第5の観点のデータ処理装置は、好ましくは、前記第1のデータ処理装置が前記記録媒体から読み出した前記コンテンツデータを一時的に記憶し、当該記憶したコンテンツデータを前記第2のデータ処理装置に出力する記憶回路とを有する。

【0046】また、本発明の第5の観点のデータ処理装置は、好ましくは、前記記憶回路は、耐振動用記憶回路の記憶領域の一部をその記憶領域とする。

【0047】また、本発明の第5の観点のデータ処理装置は、好ましくは、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第3のデータ処理装置とを有する。

【0048】また、本発明の第1の観点のデータ処理方法は、演算処理装置およびデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記データ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性の回路モジュール内で、権利書データが示す取り扱いに基づいて、当該権利書データに対応したコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定の結果を示す履歴データを生成し、前記コンテンツ鍵データを復号する。

【0049】また、本発明の第2の観点のデータ処理方法は、演算処理装置、第1のデータ処理装置および第2のデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記第1のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、前記第2のデータ処理装置は、前記演算処理装置あるいは前記第1のデータ処理装置から割り込みを受けて、マスタである前記演算処理装置あるいは前記第1のデータ処理装置のスレーブとなって、耐タンパ性のモジュール内で、前記第1のデータ

処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う。

【0050】また、本発明の第3の観点のデータ処理方法は、演算処理装置、第1のデータ処理装置および第2のデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記第1のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、前記第2のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対して読み出しおよび書き込みを行う。

【0051】また、本発明の第4の観点のデータ処理方法は、演算処理装置、第1のデータ処理装置および第2のデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記第1のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対して読み出しおよび書き込みを行い、前記第2のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う。

#### 【0052】

【発明の実施の形態】以下、本発明の実施形態に係わるEMD(Electronic Music Distribution: 電子音楽配信)システムについて説明する。

#### 第1実施形態

図1は、本実施形態のEMDシステム100の構成図である。本実施形態において、ユーザに配信されるコンテンツ(Content)データとは、情報そのものが価値を有するデジタルデータであり、以下、音楽データを例に説明する。図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ(クリアリング・ハウス、以下、ESCとも記す)102およびユーザホームネットワーク103を有する。ここで、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM105<sub>1</sub>~105<sub>4</sub>が、本発明のデータ提供装置、管理装置およびデータ処理装置にそれぞれ対応している。先ず、EMDシステム100の概要について説明する。EMDシステム100では、コンテンツプロバイダ101は、自らが提供しようとするコン

テンツのコンテンツデータCを暗号化する際に用いたコンテンツ鍵データK<sub>c</sub>、コンテンツデータCの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ106、並びに電子透かし情報の内容および埋め込み位置を示す電子透かし情報管理データを、高い信頼性のある権威機関であるEMDサービスセンタ102に送る。

【0053】EMDサービスセンタ102は、コンテンツプロバイダ101から受けたコンテンツ鍵データK<sub>c</sub>、権利書データ106並びに電子透かし情報管理データを登録(認証および権威化)する。また、EMDサービスセンタ102は、対応する期間のライセンス鍵データKD<sub>1</sub>~KD<sub>56</sub>で暗号化したコンテンツ鍵データK<sub>c</sub>、権利書データ106および自らの署名データなどを格納したキーファイルKFを作成し、これをコンテンツプロバイダ101に送る。ここで、当該署名データは、キーファイルKFの改竄の有無、キーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102において正規に登録されたことを検証するために用いられる。

【0054】また、コンテンツプロバイダ101は、コンテンツ鍵データK<sub>c</sub>でコンテンツデータCを暗号化してコンテンツファイルCFを生成し、当該生成したコンテンツファイルCFと、EMDサービスセンタ102から受けたキーファイルKFと、自らの署名データなどを格納したセキュアコンテナ(本発明のモジュール)104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などのパッケージメディアを用いて、ユーザホームネットワーク103に配給する。ここで、セキュアコンテナ104内に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【0055】ユーザホームネットワーク103は、例えば、ネットワーク機器160<sub>1</sub>およびAV機器160<sub>2</sub>~160<sub>4</sub>を有する。ネットワーク機器160<sub>1</sub>は、SAM(Secure Application Module)105<sub>1</sub>を内蔵している。AV機器160<sub>2</sub>~160<sub>4</sub>は、それぞれSAM105<sub>2</sub>~105<sub>4</sub>を内蔵している。SAM105<sub>1</sub>~105<sub>4</sub>相互間は、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルインタフェースバスなどのバス191を介して接続されている。

【0056】SAM105<sub>1</sub>~105<sub>4</sub>は、ネットワーク機器160<sub>1</sub>がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテナ104、および/または、コンテンツプロバイダ101からAV機器160<sub>2</sub>~160<sub>4</sub>に記録媒体を介してオフラインで供給されたセキュアコンテナ104に対応する期間のライセンス鍵データKD<sub>1</sub>~KD<sub>3</sub>を用いて復号した後に、署名データの検証を行う。SAM1

051 ~ 1054 に供給されたセキュアコンテナ104は、ネットワーク機器160<sub>1</sub>およびAV機器160<sub>2</sub> ~ 160<sub>4</sub>において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。SAM1051 ~ 1054は、上述したセキュアコンテナ104の購入・利用の履歴を利用履歴(Usage Log)データ108として記録すると共に、購入形態を示す利用制御データ166を作成する。利用履歴データ108は、例えば、EMDサービスセンタ102からの要求に応じて、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。利用制御データ166は、例えば、購入形態が決定される度に、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。

【0057】 EMDサービスセンタ102は、利用履歴データ108に基づいて、課金内容を決算(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行う。これにより、ユーザホームネットワーク103のユーザが決済機関91に支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101に支払われる。また、EMDサービスセンタ102は、一定期間毎に、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0058】 本実施形態では、EMDサービスセンタ102は、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有している。すなわち、EMDサービスセンタ102は、中立の立場にある最高の権威機関であるルート認証局92に対しての(ルート認証局92の下層に位置する)セカンダリ認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ101およびSAM1051 ~ 1054において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ102の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMDサービスセンタ102は、コンテンツプロバイダ101の権利書データ106を登録して権威化することも、EMDサービスセンタ102の認証機能の一つである。また、EMDサービスセンタ102は、例えば、ライセンス鍵データKD<sub>1</sub> ~ KD<sub>6</sub>などの鍵データの管理を行なう鍵データ管理機能を有する。また、EMDサービスセンタ102は、権威化した権利書データ106に記述された標準小売価格SRP(Suggested Retailer's Price)とSAM1051 ~ SAM1054から入力した利用履歴データ108とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ101に分配する権利処理(利益分配)機能を有する。

【0059】 図2は、セキュアコンテナ104の概念を

まとめた図である。図2に示すように、セキュアコンテナ104には、コンテンツプロバイダ101が作成したコンテンツファイルCFと、EMDサービスセンタ102が作成したキーファイルKFとが格納されている。コンテンツファイルCFには、ヘッダ部およびコンテンツIDを含むヘッダデータと、コンテンツ鍵データKcを用いた暗号化されたコンテンツデータCと、これらについてのコンテンツプロバイダ101の秘密鍵データKcp,sを用いた署名データとが格納されている。キーファイルKFには、ヘッダ部およびコンテンツIDを含むヘッダデータと、ライセンス鍵データKD<sub>1</sub> ~ KD<sub>6</sub>によって暗号化されたコンテンツ鍵データKcおよび権利書データ106と、これらについてのEMDサービスセンタ102の秘密鍵データKesc,sによる署名データとが格納されている。なお、図2において、権利書データ106は、ライセンス鍵データによって暗号化されていなくてもよい。但し、この場合でも、権利書データ106には、コンテンツプロバイダ101の秘密鍵データKcp,sを用いた署名データを付加する。

【0060】 以下、EMDシステム100の各構成要素について詳細に説明する。

〔コンテンツプロバイダ101〕 コンテンツプロバイダ101は、EMDサービスセンタ102との間で通信を行う前に、例えば、自らが生成した公開鍵データKcp,p、自らの身分証明書および銀行口座番号(決済を行う口座番号)をオンラインでEMDサービスセンタ102に登録し、自らの識別子(識別番号)CP\_IDを得る。また、コンテンツプロバイダ101は、EMDサービスセンタ102から、EMDサービスセンタ102の公開鍵データKesc,pと、ルート認証局92の公開鍵データKrc-a,pとを受ける。

【0061】 コンテンツプロバイダ101は、図3(A)に示すコンテンツファイルCFと、当該コンテンツファイルCFの署名データSIG<sub>6</sub>,cpと、キーファイルデータベース118bから読み出した当該コンテンツファイルCFに対応する図3(B)に示すキーファイルKFと、当該キーファイルKFの署名データSIG<sub>7</sub>,cpと、記憶部119から読み出したコンテンツプロバイダ101の公開鍵証明書データCERcpと、当該公開鍵証明書データCERcpの署名データSIG<sub>1</sub>,escとを格納したセキュアコンテナ104を生成する。また、コンテンツプロバイダ101は、セキュアコンテナ104をオンラインあるいはオフラインで、図1に示すユーザホームネットワーク103のネットワーク機器160<sub>1</sub>に供給する。このように、本実施形態では、コンテンツプロバイダ101の公開鍵データKcp,pの公開鍵証明書CERcpをセキュアコンテナ104に格納してユーザホームネットワーク103に送信するイン・バンド(In-band)方式を採用している。従って、ユーザホームネットワーク103は、公開鍵証明書CERcpを得るための通信を



EMDサービスセンタ102との間で行う必要がない。  
なお、本発明では、公開鍵証明書CERcpをセキュアコンテナ104に格納しないで、ユーザホームネットワーク103がEMDサービスセンタ102から公開鍵証明書CERcpを得るアウト・オブ・バンド(Out-Of-Band)方式を採用してもよい。

【0062】なお、本実施形態では、署名データは、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM1051~1054の各々において、署名を行なう対象となるデータのハッシュ値をとり、自らの秘密鍵データKcp, s, KESC, KSAM1~KSAM4を用いて作成される。ここで、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値(出力)から入力予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化した場合、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探索することが困難であるという特徴を有している。

【0063】以下、セキュアコンテナ104内の各データについて詳細に説明する。

<署名データSIG6, cp>署名データSIG6, cpは、セキュアコンテナ104の受信先において、コンテンツファイルCFの作成者および送信者の正当性を検証するために用いられる。

<署名データSIG7, cp>署名データSIG7, cpは、セキュアコンテナ104の受信先において、キーファイルKFの送信者の正当性を検証するために用いられる。なお、セキュアコンテナ104の受信先において、キーファイルKFの作成者の正当性の検証は、キーファイルKF内の署名データSIGK1, ESCに基づいて行われる。また、署名データSIGK1, ESCは、キーファイルKFが、EMDサービスセンタ102に登録されているか否かを検証するためにも用いられる。

【0064】<コンテンツファイルCF>図4は、図3(A)に示すコンテンツファイルCFをさらに詳細に説明するための図である。コンテンツファイルCFは、図3(A)および図4に示すように、ヘッダデータと、暗号化部114から入力したそれぞれコンテンツ鍵データKcで暗号化されたメタデータMeta、コンテンツデータC、A/V伸長用ソフトウェアおよび電子透かし情報モジュール(Watermark Module)WMとを格納している。なお、図3(A)は、コンテンツデータCを伸長するA/V圧縮伸長用装置として、DSP(Digital Signal Processor)を用いた場合のコンテンツファイルCFの構成である。当該DSPでは、セキュアコンテナ104内のA/V伸長用ソフトウェアおよび電子透かし情報モジュールを用いて、セキュアコンテナ104内のコンテンツデータCの伸長および電子透かし情報の埋め込

みおよび検出を行う。そのため、コンテンツプロバイダ101は任意の圧縮方式および電子透かし情報の埋め込み方式を採用できる。A/V圧縮伸長用装置としてA/V伸長処理および電子透かし情報の埋め込み・検出処理をハードウェアあるいは予め保持されたソフトウェアを用いて行う場合には、コンテンツファイルCF内にA/V伸長用ソフトウェアおよび電子透かし情報モジュールを格納しなくてもよい。

【0065】ヘッダデータには、図4に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データKcp, sによる署名データ、ディレクトリ情報、ハイパーリンク情報、シリアルナンバー、コンテンツファイルCFの有効期限並びに作成者情報、ファイルサイズ、暗号の有無、暗号アルゴリズム、署名アルゴリズムに関する情報、およびディレクトリ情報などに関するコンテンツプロバイダ101の秘密鍵データKcp, sによる署名データが含まれる。

【0066】メタデータMetaには、図4に示すように、商品(コンテンツデータC)の説明文、商品デモ宣伝情報、商品関連情報およびこれらについてのコンテンツプロバイダ101による署名データが含まれる。本発明では、図3(A)および図4に示すように、コンテンツファイルCF内にメタデータMetaを格納して送信する場合を例示するが、メタデータMetaをコンテンツファイルCF内に格納せずに、コンテンツファイルCFを送信する経路とは別の経路でコンテンツプロバイダ101からSAM1051などに送信してもよい。

【0067】コンテンツデータCは、例えば、コンテンツマスタソースデータベースから読み出したコンテンツデータに対して、ソース電子透かし情報(Source Watermark)Ws、コピー管理用電子透かし情報(Copy Control Watermark)Wc、ユーザ電子透かし情報(User Watermark)Wuおよびリンク用電子透かし情報(Link Watermark)WLなどを埋め込んだ後に、例えば、ATRAC3(Adaptive Transform Acoustic Coding 3)(商標)などの音声圧縮方式で圧縮され、その後、コンテンツ鍵データKcを共通鍵として用い、DES(Data Encryption Standard)やTriple DESなどの共通鍵暗号化方式で暗号化されたデータである。ここで、コンテンツ鍵データKcは、例えば、乱数発生器を用いて所定ビット数の乱数を発生して得られる。なお、コンテンツ鍵データKcは、コンテンツデータCが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データKcは、例えば、所定時間毎に更新される。また、複数のコンテンツプロバイダ101が存在する場合に、個々のコンテンツプロバイダ101によって固有のコンテンツ鍵データKcを用いてもよいし、全てのコンテンツプロバイダ101に共通のコンテンツ鍵データKcを用いてもよい。

【0068】ソース電子透かし情報Wsは、コンテンツ

データの著作権者名、ISRCコード、オーサリング日付、オーサリング機器ID(Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報Wcは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Wuには、例えば、セキュアコンテナ104の配給元および配給先を特定するためのコンテンツプロバイダ101の識別子CP\_\_IDおよびユーザホームネットワーク103のSAM105\_1~105\_4の識別子SAM\_\_ID\_1~SAM\_\_ID\_4が含まれる。リンク用電子透かし情報(Link Watermark)WLは、例えば、コンテンツデータCのコンテンツIDを含んでいる。リンク用電子透かし情報WLをコンテンツデータCに埋め込むことで、例えば、テレビジョンやAM/FMラジオなどのアナログ放送でコンテンツデータCが配信された場合でも、ユーザからの要求に応じて、EMDサービスセンタ102は、当該コンテンツデータCを扱っているコンテンツプロバイダ101をユーザに紹介できる。すなわち、当該コンテンツデータCの受信先において、電子透かし情報デコーダを利用したコンテンツデータCに埋め込まれたリンク用電子透かし情報WLを検出し、当該検出したリンク用電子透かし情報WLに含まれるコンテンツIDをEMDサービスセンタ102に送信することで、EMDサービスセンタ102は当該ユーザに対して、当該コンテンツデータCを扱っているコンテンツプロバイダ101などを紹介できる。

【0069】具体的には、例えば、車の中でユーザがラジオを聞きながら、放送中の曲が良いとユーザが思った時点で、所定のボタンを押せば、当該ラジオに内蔵されている電子透かし情報デコーダが、当該コンテンツデータCに埋め込まれているリンク用電子透かし情報WLに含まれるコンテンツIDや当該コンテンツデータCを登録しているEMDサービスセンタ102の通信アドレスなどを検出し、当該検出したデータをメモリスティックなどの半導体メモリやMD(Mini Disk)などの光ディスクなどの可搬メディアに搭載されているメディアSAMに記録する。そして、当該可搬メディアをネットワークに接続されているSAMを搭載したネットワーク機器をセットする。そして、当該SAMとEMDサービスセンタ102とが相互認証を行った後に、メディアSAMに搭載されている個人情報と、上記記録したコンテンツIDなどをネットワーク機器からEMDサービスセンタ102に送信する。その後、ネットワーク機器に、当該コンテンツデータCを扱っているコンテンツプロバイダ101などの紹介リストなどを、EMDサービスセンタ102から受信する。また、その他に、例えば、EMDサービスセンタ102が、ユーザからコンテンツIDなどを受信したときに、当該コンテンツIDに対応したコンテンツデータCを提供しているコンテンツプロバイダ

101に当該ユーザを特定した情報を通知してもよい。この場合に、当該通信を受けたコンテンツプロバイダ101は、当該ユーザが契約者であれば、当該コンテンツデータCをユーザのネットワーク機器に送信し、当該ユーザが契約者でなければ、自らに関するプロモーション情報をユーザのネットワーク機器に送信してもよい。

【0070】また、後述する第2実施形態では、リンク用電子透かし情報WLに基づいて、EMDサービスセンタ102は、ユーザに、当該コンテンツデータCを扱っているサービスプロバイダ310を紹介できる。

【0071】また、本実施形態では、好ましくは、各々の電子透かし情報の内容と埋め込み位置とを、電子透かし情報モジュールWMとして定義し、EMDサービスセンタ102において電子透かし情報モジュールWMを登録して管理する。電子透かし情報モジュールWMは、例えば、ユーザホームネットワーク103内のネットワーク機器160\_1およびAV機器160\_2~160\_4が、電子透かし情報の正当性を検証する際に用いられる。例えば、ユーザホームネットワーク103では、EMDサービスセンタ102が管理するユーザ電子透かし情報モジュールに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【0072】A/V伸長用ソフトウェアSoftは、ユーザホームネットワーク103のネットワーク機器160\_1およびAV機器160\_2~160\_4において、コンテンツファイルCFを伸長する際に用いられるソフトウェアであり、例えば、ATRAC3方式の双方用ソフトウェアである。このように、セキュアコンテナ104内にA/V伸長用ソフトウェアSoftを格納することで、SAM105\_1~105\_4においてセキュアコンテナ104内に格納されたA/V伸長用ソフトウェアSoftを用いてコンテンツデータCの伸長を行うことができ、コンテンツデータC毎あるいはコンテンツプロバイダ101毎にコンテンツデータCの圧縮および伸長方式をコンテンツプロバイダ101が自由に設定しても、ユーザに多大な負担をかけることはない。

【0073】また、コンテンツファイルCFには、図4に示すように、ファイルリダと、秘密鍵データK<sub>ep,S</sub>によるファイルリダの署名データとを含むようにしてもよい。このようにすることで、SAM105\_1~105\_4において、異系列の複数のセキュアコンテナ104から受信したそれぞれ異なるフォーマットのコンテンツファイルCFを格納した複数のセキュアコンテナ104を効率的に処理できる。

【0074】ここで、ファイルリダは、コンテンツファイルCFおよびそれに対応するキーファイルKFを読む際に用いられ、これらのファイルの読み込み手順など

を示している。但し、本実施形態では、EMDサービスセンタ102からSAM105<sub>1</sub>～105<sub>4</sub>に、当該ファイルリダを予め送信している場合を例示する。すなわち、本実施形態では、セキュアコンテナ104のコンテンツファイルCFは、ファイルリダを格納していない。

【0075】本実施形態では、コンテンツデータCの圧縮方式、圧縮の有無、暗号化方式（共通鍵暗号化方式および公開鍵暗号化方式の何れの場合も含む）、コンテンツデータCを得た信号の諸元（サンプリング周波数など）および署名データの作成方式（アルゴリズム）に依存しない形式で、暗号化されたコンテンツデータCがセキュアコンテナ104内に格納されている。すなわち、これらの事項をコンテンツプロバイダ101が自由に決定できる。

【0076】＜キーファイルKF＞図5は、図3（A）に示すキーファイルKFを詳細に説明するための図である。本実施形態では、例えば、図6に示すように、コンテンツプロバイダ101からEMDサービスセンタ102に登録用モジュールMod<sub>2</sub>が送られて登録処理が行われた後に、例えば6カ月分のキーファイルKFがEMDサービスセンタ102からコンテンツプロバイダ101に送られ、キーファイルデータベースに格納される。このとき、登録用モジュールMod<sub>2</sub>およびキーファイルKFの送受信時に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証およびセッション鍵データK<sub>SES</sub>による暗号化および復号が行われる。キーファイルKFは、コンテンツデータC毎に存在し、後述するように、コンテンツファイルCFのヘッダ内のディレクトリ構造データDSDによって、対応するコンテンツファイルCFとの間でリンク関係が指定されている。キーファイルKFには、図3（B）および図5に示すように、ヘッダ、コンテンツ鍵データK<sub>c</sub>、権利書データ（使用許諾条件）106、SAMプログラム・ダウンロード・コンテナSDC<sub>1</sub>～SDC<sub>3</sub>および署名データSIG<sub>K1,ESC</sub>が格納されている。ここで、コンテンツプロバイダ101の秘密鍵データK<sub>ESC</sub>を用いた署名データは、図3（B）に示すようにキーファイルKFに格納される全てのデータに対しての署名データ

K<sub>1,ESC</sub>にしてもよいし、図5に示すようにヘッダから鍵ファイルに関する情報までのデータに対しての署名データと、コンテンツ鍵データK<sub>c</sub>および権利書データ106に対しての署名データと、SAMプログラム・ダウンロード・コンテナSDC<sub>1</sub>～SDC<sub>3</sub>に対しての署名データとを別々に設けてもよい。コンテンツ鍵データK<sub>c</sub>および権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC<sub>1</sub>～SDC<sub>3</sub>とは、それぞれ対応する期間のライセンス鍵データKD<sub>1</sub>～KD<sub>6</sub>を用いて暗号化されている。なお、権利書データ106は、キーファイルKF内に格納しないでもよい。この場合には、例えば、

権利書データ106はライセンス鍵データによる暗号化を行わずに、署名データを付加する。

【0077】ヘッダデータには、図5に示すように、同期信号、コンテンツID、コンテンツIDに対してのコンテンツプロバイダ101の秘密鍵データK<sub>ESC</sub>、Sによる署名データ、ディレクトリ構造データ、ハイパーリンクデータ、キーファイルKFに関する情報、およびディレクトリ構造データ等に対してのコンテンツプロバイダ101の秘密鍵データK<sub>ESC</sub>、Sによる署名データが含まれる。なお、ヘッダデータに含める情報としては種々の情報が考えられ、状況に応じて任意に変更可能である。例えば、ヘッダデータに、図7に示すような情報を含めてもよい。また、コンテンツIDには、例えば、図8に示す情報が含まれている。コンテンツIDは、EMDサービスセンタ102あるいはコンテンツプロバイダ101において作成され、EMDサービスセンタ102において作成された場合には図8に示すようにEMDサービスセンタ102の秘密鍵データK<sub>ESC</sub>、Sによる署名データが添付され、コンテンツプロバイダ101において作成された場合にはコンテンツプロバイダ101の秘密鍵データK<sub>CP</sub>、Sが添付される。コンテンツIDは、コンテンツプロバイダ101およびEMDサービスセンタ102の何れで作成してもよい。

【0078】ディレクトリ構造データは、セキュアコンテナ104内におけるコンテンツファイルCF相互間の対応関係と、コンテンツファイルCFとキーファイルKFとの対応関係を示している。例えば、セキュアコンテナ104内にコンテンツファイルCF<sub>1</sub>～CF<sub>3</sub>と、それらに対応するキーファイルKF<sub>1</sub>～KF<sub>3</sub>が格納されている場合には、10図9に示すように、コンテンツファイルCF<sub>1</sub>～CF<sub>3</sub>相互間のリンクと、コンテンツファイルCF<sub>1</sub>～CF<sub>3</sub>とキーファイルKF<sub>1</sub>～KF<sub>3</sub>との間のリンク関係とがディレクトリ構造データによって確立される。ハイパーリンクデータは、セキュアコンテナ104の内外の全てのファイルを対象として、キーファイルKF相互間の階層構造と、コンテンツファイルCFとキーファイルKFとの対応関係を示している。具体的には、図10に示すように、セキュアコンテナ104内にコンテンツファイルCFおよびキーファイルKF毎のリンク先のアドレス情報とその認証値（ハッシュ値）とを格納し、ハッシュ関数H（x）を用いて得た自らのアドレス情報のハッシュ値と、相手方の認証値とを比較してリンク関係を検証する。

【0079】また、権利書データ106は、コンテンツデータCの運用ルールを定義した記述子（ディスクリプター）であり、例えば、コンテンツプロバイダ101の運用者が希望する卸売価格やコンテンツデータCの複製ルールなどが記述されている。具体的には、権利書データ106には、図5に示すように、コンテンツID、コンテンツプロバイダ101の識別子CP\_ID、権利書

データ106の有効期限、EMDサービスセンタ102の通信アドレス、利用空間調査情報、卸売価格情報SRP(Suggested Retailer Price)、取扱方針、取扱制御情報(Usage Control)、商品デモ(試験)の取扱制御情報およびそれらについての署名データなどが含まれる。

ここで、取扱制御情報は、例えば、再配付(Re-Distribution)、再生課金(Pay Per Use)、完全買い切り(Sell Through)、時間制限買い切り(Time Limited Sell Through)、回数制限買い切り(Shell Through Pay Per Play N)、時間課金(Pay Per Time)、SCMS機器への再生課金、ブロック課金(Pay Per Block)などの購入形態のうち許諾された購入形態を示す情報である。

【0080】なお、後述する第2実施形態のように、サブスプロバイダ310を介してユーザホームネットワーク303にセキュアコンテンツ304を送信する場合には、権利書データ106には、コンテンツプロバイダ301がセキュアコンテンツ104を提供するサブスプロバイダ310の識別子SP\_IDが含まれる。

【0081】また、SAMプログラム・ダウンロード・コンテンツSDC<sub>1</sub>～SDC<sub>3</sub>には、図5に示すように、SAM105<sub>1</sub>～105<sub>4</sub>内でプログラムのダウンロードを行う際に用いられるダウンロードの手順を示すダウンロード・ドライバと、権利書データ(UCP)U106のシンタックス(文法)を示すUCP-L(Label)

・R(Reader)などのラベルリーダと、SAM105<sub>1</sub>～105<sub>4</sub>に内蔵された記憶部192(マスクROM1104、不揮発性メモリ1105などのフラッシュROM)の書き換えおよび消去をブロック単位でロック状態/非ロック状態にするためのロック鍵データと、それらについての署名データとが含まれる。SAM105<sub>1</sub>～105<sub>4</sub>のマスクROM1104および不揮発性メモリ1105では、ロック鍵データに基づいて、記憶データの書き換えおよび消去を許可するか否かをブロック単位で制御する。

【0082】以下、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテンツ104を供給する形態について説明する。コンテンツプロバイダ101は、前述したように、セキュアコンテンツ104を、オフラインおよび/またはオンラインでユーザホームネットワーク103に供給する。コンテンツプロバイダ101は、オンラインで、セキュアコンテンツ104をユーザホームネットワーク103のネットワーク機器160<sub>1</sub>に供給する場合には、ネットワーク機器160<sub>1</sub>との間で相互認証を行ってセッション鍵(共通鍵)データK<sub>SES</sub>を共有し、セキュアコンテンツ104を当該セッション鍵データK<sub>SES</sub>を用いて暗号化してEMDサービスセンタ102に送信する。セッション鍵データK<sub>SES</sub>は、相互認証を行う度に新たに生成される。このとき、セキュアコンテンツ104を送信する通信プロトコルとして、デジタル放送であればMHEG(Multimedia an

d Hypermedia information coding Experts Group)プロトコルを用い、インターネットであればXML/SMIL/H TML(Hyper TextMarkup Language)を用い、これらの通信プロトコル内に、セキュアコンテンツ104を、符号化方式に依存しない形式でトンネリングして埋め込む。従って、通信プロトコルとセキュアコンテンツ104との間でフォーマットの整合性をとる必要性はなく、セキュアコンテンツ104のフォーマットを柔軟に設定できる。なお、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテンツ104を送信する際に用いる通信プロトコルは、上述したものには限定されず任意である。本実施形態では、コンテンツプロバイダ101、EMDサービスセンタ102およびネットワーク機器160<sub>1</sub>に内蔵された相互間で通信を行うためのモジュールとして、例えば、内部の処理内容の監視(モニタリング)および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0083】また、コンテンツプロバイダ101は、オフラインで、セキュアコンテンツ104をユーザホームネットワーク103に供給する場合には、以下に示すようなROM型あるいはRAM型の記録媒体にセキュアコンテンツ104を記録して、当該記録媒体を所定の流通経路を経てユーザホームネットワーク103に供給する。図11は、本実施形態で用いられるROM型の記録媒体130<sub>1</sub>を説明するための図である。図11に示すように、ROM型の記録媒体130<sub>1</sub>は、ROM領域131、セキュアRAM領域132およびメディアSAM133を有する。ROM領域131には、図3(A)に示したコンテンツファイルCFが記憶されている。また、セキュアRAM領域132は、記憶データに対してのアクセスに所定の許可(認証)が必要な領域であり、図3(B)、(C)に示したキーファイルKFおよび公開鍵証明書データCERcpと機器の種類に応じて固有の値を持つ記録用鍵データKSTRとを引数としてMAC(Message Authentication Code)関数を用いて生成した署名データと、当該キーファイルKFおよび公開鍵証明書データCERcpとを記録媒体に固有の値を持つメディア鍵データK<sub>MED</sub>を用いて暗号化したデータとが記憶される。また、セキュアRAM領域132には、例えば、不正行為などで無効となったコンテンツプロバイダ101およびSAM105<sub>1</sub>～105<sub>5</sub>を特定する公開鍵証明書破棄データ(リボケーションリスト)が記憶される。本実施形態で用いられるメディアSAMおよび後述するメディア・ドラブSAM260では、これら相互間で通信を行う際に、自らが持つリボケーションリストと相手方が持つリボケーションリストの作成時を比較し、自らが持つリボケーションリストの作成時が前の場合には、相手方が持つリボケーションリストによって自らのリボケーションリストを更新する。また、セキュアRAM領域

132には、後述するようにユーザホームネットワーク103のSAM105<sub>1</sub>～105<sub>4</sub>においてコンテンツデータCの購入・利用形態が決定されたときに生成される利用制御状態(UCS)データ166などが記憶される。これにより、利用制御データ166がセキュアRAM領域132に記憶されることで、購入・利用形態が決定したROM型の記録媒体130<sub>1</sub>となる。メディアSAM133には、例えば、ROM型の記録媒体130<sub>1</sub>の識別子であるメディアIDと、メディア鍵データK<sub>MED</sub>とが記憶されている。メディアSAM133は、例えば、相互認証機能を有している。

【0084】本実施形態で用いるROM型の記録媒体としては、例えば、図11に示すものの他に、図12に示すROM型の記録媒体130<sub>2</sub>および図13に示すROM型の記録媒体130<sub>3</sub>なども考えられる。図12に示すROM型の記録媒体130<sub>2</sub>は、ROM領域131と認証機能を有するメディアSAM133とを有し、図11に示すROM型の記録媒体130<sub>1</sub>のようにセキュアRAM領域132を備えていない。ROM型の記録媒体130<sub>2</sub>を用いる場合には、ROM領域131にコンテンツファイルCFを記録し、メディアSAM133にキーファイルKFを記憶する。また、図13に示すROM型の記録媒体130<sub>3</sub>は、ROM領域131およびセキュアRAM領域132を有し、図11に示すROM型の記録媒体130<sub>1</sub>のようにメディアSAM133を有していない。ROM型の記録媒体130<sub>3</sub>を用いる場合には、ROM領域131にコンテンツファイルCFを記録し、セキュアRAM領域132にキーファイルKFを記録する。また、ROM型の記録媒体130<sub>3</sub>を用いる場合には、SAMとの間で相互認証は行わない。また、本実施形態ではROM型の記録媒体の他にRAM型の記録媒体も用いられる。

【0085】本実施形態で用いるRAM型の記録媒体としては、例えば図14に示すように、メディアSAM133、セキュアRAM領域132およびセキュアでないRAM領域134を有するRAM型の記録媒体130<sub>4</sub>がある。RAM型の記録媒体130<sub>4</sub>では、メディアSAM133は認証機能を持ち、キーファイルKFを記憶する。また、RAM領域134には、コンテンツファイルCFが記録される。また、本実施形態で用いるRAM型の記録媒体としては、その他に、図15に示すRAM型の記録媒体1350<sub>5</sub>および図16に示すRAM型の記録媒体130<sub>6</sub>なども考えられる。図15に示すRAM型の記録媒体130<sub>5</sub>は、セキュアでないRAM領域134と認証機能を有するメディアSAM133とを有し、図14に示すRAM型の記録媒体130<sub>4</sub>のようにセキュアRAM領域132を備えていない。RAM型の記録媒体130<sub>5</sub>を用いる場合には、RAM領域134にコンテンツファイルCFを記録し、メディアSAM133にキーファイルKFを記憶する。また、図16に示

すRAM型の記録媒体130<sub>6</sub>は、セキュアRAM領域132およびセキュアでないRAM領域134を有し、図14に示すRAM型の記録媒体130<sub>4</sub>のようにメディアSAM133を有していない。RAM型の記録媒体130<sub>6</sub>を用いる場合には、RAM領域134にコンテンツファイルCFを記録し、セキュアRAM領域132にキーファイルKFを記録する。また、RAM型の記録媒体130<sub>6</sub>を用いる場合には、SAMとの間で相互認証は行わない。

【0086】ここで、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配信は、上述したように記録媒体130<sub>1</sub>を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ106が格納された共通の形式のセキュアコンテナ104を用いる。従って、ユーザホームネットワーク103のSAM105<sub>1</sub>～105<sub>4</sub>では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ106に基づいた権利処理を行なうことができる。

【0087】また、上述したように、本実施形態では、セキュアコンテナ104内に、コンテンツ鍵データK<sub>c</sub>で暗号化されたコンテンツデータCと、当該暗号化を解くためのコンテンツ鍵データK<sub>c</sub>とを同封するイン・バンド(In-Band)方式を採用している。イン・バンド方式では、ユーザホームネットワーク103の機器で、コンテンツデータCを再生しようとするときに、コンテンツ鍵データK<sub>c</sub>を別途配信する必要がある。ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データK<sub>c</sub>はライセンス鍵データKD<sub>1</sub>～KD<sub>6</sub>で暗号化されているが、ライセンス鍵データKD<sub>1</sub>～KD<sub>6</sub>は、EMDサービスセンタ102で管理されており、ユーザホームネットワーク103のSAM105<sub>1</sub>～105<sub>5</sub>に事前に{SAM105<sub>1</sub>～105<sub>4</sub>}がEMDサービスセンタ102に初回にアクセスする際に)配信されているので、ユーザホームネットワーク103では、EMDサービスセンタ102との間をオンラインで接続することなく、オフラインで、コンテンツデータCの利用が可能になる。なお、本発明は、後述するようにコンテンツデータCとコンテンツ鍵データK<sub>c</sub>とを別々に、ユーザホームネットワーク103に供給するアウト・オブ・バンド(Out-Of-Band)方式を採用できる柔軟性を有している。

【0088】以下、コンテンツプロバイダ101におけるセキュアコンテナ104の作成に係る処理の流れを説明する。図17、図18、図19は、当該処理の流れを説明するためのフローチャートである。ステップS17-1:コンテンツプロバイダ101の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ102に登録処理を行い、グローバルユニーク

な識別子CP\_IDを得ている。また、コンテンツプロバイダ101は、予め自らの公開鍵証明書データCERcpをEMDサービスセンタ102から得ている。

ステップS17-2: コンテンツプロバイダ101は、新しくオーサリングするコンテンツデータや、既に保管されているレガシーコンテンツデータなどのコンテンツマスタソースをデジタル化し、さらにコンテンツIDを割り振り、コンテンツマスタソースデータベースに格納して一元的に管理する。

ステップS17-3: コンテンツプロバイダ101は、ステップS17-2において一元的に管理した各々のコンテンツマスタソースにメタデータMetaを作成し、これをメタデータデータベースに格納して管理する。

【0089】ステップS17-4: コンテンツプロバイダ101は、コンテンツマスタソースデータベースからコンテンツマスタソースであるコンテンツデータを読み出して電子透かし情報を埋め込む。

ステップS17-5: コンテンツプロバイダ101は、ステップS17-4で埋め込んだ電子透かし情報の内容と埋め込み位置とを所定のデータベースに格納する。

ステップS17-6: 電子透かし情報が埋め込まれたコンテンツデータを圧縮する。

ステップS17-7: コンテンツプロバイダ101は、ステップS17-6で圧縮したコンテンツデータを伸長してコンテンツデータを作成する。

ステップS17-8: コンテンツプロバイダ101は、伸長したコンテンツデータの聴覚検査を行う。

ステップS17-9: コンテンツプロバイダ101は、コンテンツデータに埋め込まれた電子透かし情報を、ステップS17-5でデータベースに格納した埋め込み内容および埋め込み位置に基づいて検出する。そして、コンテンツプロバイダ101は、聴覚検査および電子透かし情報の検出の双方が成功した場合には、ステップS17-10の処理を行い、何れか一方が失敗した場合にはステップS17-4の処理を繰り返す。

【0090】ステップS17-10: コンテンツプロバイダ101は、乱数を発生してコンテンツ鍵データKcを生成し、これを保持する。また、コンテンツプロバイダ101は、ステップS17-6で圧縮したコンテンツデータを、コンテンツ鍵データKcを用いて暗号化する。

【0091】ステップS17-11: コンテンツプロバイダ101は、図3(A)に示すコンテンツファイルCFを作成し、これをコンテンツファイルデータベースに格納する。

【0092】ステップS17-12: コンテンツプロバイダ101は、コンテンツデータCについての権利書データ106を作成する。

ステップS17-13: コンテンツプロバイダ101は、SRPを決定する。

ステップS17-14: コンテンツプロバイダ101は、コンテンツID、コンテンツ鍵データKcおよび権利書データ106をEMDサービスセンタ102に出力する。

ステップS17-15: コンテンツプロバイダ101は、ライセンス鍵データKD<sub>1</sub>〜KD<sub>3</sub>で暗号化されたキーファイルKFをEMDサービスセンタ102から入力する。

ステップS17-16: コンテンツプロバイダ101は、入力したキーファイルKFをキーファイルデータベースに格納する。

【0093】ステップS17-17: コンテンツプロバイダ101は、コンテンツファイルCFとキーファイルKFとのリンク関係をハイパーリンクで結ぶ。

ステップS17-18: コンテンツプロバイダ101は、コンテンツファイルCFのハッシュ値をとり、秘密鍵データKcp,sを用いて署名データSIG<sub>6</sub>,cpを生成する。また、コンテンツプロバイダ101は、キーファイルKFのハッシュ値をとり、秘密鍵データKcp,sを用いて署名データSIG<sub>7</sub>,cpを生成する。

【0094】ステップS17-19: コンテンツプロバイダ101は、図3に示すように、コンテンツファイルCF、キーファイルKF、公開鍵証明書データCERcp、署名データSIG<sub>6</sub>,cp, SIG<sub>7</sub>,cp, SIG<sub>1</sub>,ESCを格納したセキュアコンテナ104を作成する。

【0095】ステップS17-20: 複数のセキュアコンテナを用いたコンボジット形式でコンテンツデータを提供する場合には、ステップS17-1〜B19の処理を繰り返して各々のセキュアコンテナ104を作成し、コンテンツファイルCFとキーファイルKFとの間のリンク関係と、コンテンツファイルCF相互間のリンク関係とをハイパーリンクなどを用いて結ぶ。

ステップS17-21: コンテンツプロバイダ101は、作成したセキュアコンテナ104をセキュアコンテナデータベースに格納する。

【0096】[EMDサービスセンタ102] 図20は、EMDサービスセンタ102の主な機能を示す図である。EMDサービスセンタ102は、主に、図20に示すように、ライセンス鍵データをコンテンツプロバイダ101およびSAM105<sub>1</sub>〜105<sub>4</sub>に供給する処理と、公開鍵証明書データCERcp, CERSAM<sub>1</sub>〜CERSAM<sub>4</sub>の発行処理と、キーファイルKFの発行処理、利用履歴データ108に基づいた決済処理(利益分配処理)とを行う。

【0097】<ライセンス鍵データの供給処理>まず、EMDサービスセンタ102からユーザホームネットワーク103内のSAM105<sub>1</sub>〜105<sub>4</sub>にライセンス鍵データを送信する際の処理の流れを説明する。EMDサービスセンタ102では、所定期間毎に、例えば、3カ月分のライセンス鍵データKD<sub>1</sub>〜KD<sub>3</sub>を鍵データ

ベースから読み出して、各々のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK<sub>ESC,S</sub>を用いて、それぞれに対応する署名データS<sub>IGKD1,ESC</sub>~S<sub>IGKD3,ESC</sub>を作成する。そして、EMDサービスセンタ102は、3カ月分のライセンス鍵データKD<sub>1</sub>~KD<sub>3</sub>およびそれらの署名データS<sub>IGKD1,ESC</sub>~S<sub>IGKD3,ESC</sub>を、SAM1051~1054と間の相互認証で得られたセッション鍵データK<sub>SES</sub>を用いて暗号化した後に、SAM1051~1054に送信する。また、同様に、EMDサービスセンタ102は、コンテンツプロバイダ101に、例えば、6カ月分のライセンス鍵データKD<sub>1</sub>~KD<sub>6</sub>を送信する。

【0098】＜公開鍵証明書データの発行処理＞次に、EMDサービスセンタ102がコンテンツプロバイダ101から、公開鍵証明書データCER<sub>CP</sub>の発行要求を受けた場合の処理を説明する。EMDサービスセンタ102は、コンテンツプロバイダ101の識別子C<sub>P\_ID</sub>、公開鍵データK<sub>CP</sub>、および署名データS<sub>IGG,CP</sub>をコンテンツプロバイダ101から受信すると、これらを、コンテンツプロバイダ101と間の相互認証で得られたセッション鍵データK<sub>SES</sub>を用いて復号する。そして、当該復号した署名データS<sub>IGG,CP</sub>の正当性を検証した後に、識別子C<sub>P\_ID</sub>および公開鍵データK<sub>CP</sub>に基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ101がC<sub>P</sub>データベースに登録されているか否かを確認する。そして、EMDサービスセンタ102は、当該コンテンツプロバイダ101のX.509形式の公開鍵証明書データCER<sub>CP</sub>を証明書データベースから読み出し、公開鍵証明書データCER<sub>CP</sub>のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK<sub>ESC,S</sub>を用いて、署名データS<sub>IGL,ESC</sub>を作成する。そして、EMDサービスセンタ102は、公開鍵証明書データCER<sub>CP</sub>およびその署名データS<sub>IGL,ESC</sub>を、コンテンツプロバイダ101と間の相互認証で得られたセッション鍵データK<sub>SES</sub>を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0099】なお、EMDサービスセンタ102がSAM1051から、公開鍵証明書データCER<sub>SAM1</sub>の発行要求を受けた場合の処理も、SAM1051と間の処理が行われる点を除いて、公開鍵証明書データCER<sub>CP</sub>の発行要求を受けた場合の処理と同じである。公開鍵証明書データCER<sub>CP</sub>も、X.509形式で記述されている。なお、本発明では、EMDサービスセンタ102は、例えば、SAM1051の出荷時に、SAM1051の秘密鍵データK<sub>SAM1</sub>、および公開鍵データK<sub>SAM1,P</sub>をSAM1051の記憶部に記憶する場合には、当該出荷時に、公開鍵データK<sub>SAM1,P</sub>の公開鍵証明書データCER<sub>SAM1</sub>を作成してもよい。このとき、当該出荷時に、公開鍵証明書データCER<sub>SAM1</sub>を、SAM1051の記

憶部に記憶してもよい。

【0100】＜キーファイルKFの発行処理＞EMDサービスセンタ102は、コンテンツプロバイダ101から図6に示す登録用モジュールM<sub>od2</sub>を受信すると、コンテンツプロバイダ101と間の相互認証で得られたセッション鍵データK<sub>SES</sub>を用いて登録用モジュールM<sub>od2</sub>を復号する。そして、EMDサービスセンタ102は、鍵データベースから読み出した公開鍵データK<sub>CP,P</sub>を用いて、署名データS<sub>IGM1,CP</sub>の正当性を検証する。次に、EMDサービスセンタ102は、登録用モジュールM<sub>od2</sub>に格納された権利書データ106、コンテンツ鍵データK<sub>c</sub>、電子透かし情報管理データWMおよびSRPを、権利書データベースに登録する。

【0101】次に、EMDサービスセンタ102は、鍵データベースから読み出した対応する期間のライセンス鍵データKD<sub>1</sub>~KD<sub>6</sub>を用いて、コンテンツ鍵データK<sub>c</sub>および権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC<sub>1</sub>~SDC<sub>3</sub>とを暗号化する。次に、EMDサービスセンタ102は、ヘッダデータと、コンテンツ鍵データK<sub>c</sub>および権利書データ106と、SAMプログラム・ダウンロード・コンテナSDC<sub>1</sub>~SDC<sub>3</sub>との全体に対してハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK<sub>ESC,S</sub>を用いて署名データS<sub>IGK1,ESC</sub>を作成する。次に、EMDサービスセンタ102は、図3(B)に示すキーファイルKFを作成し、これをKFデータベースに格納する。次に、EMDサービスセンタ102は、KFデータベースにアクセスを行って得たキーファイルKFを、コンテンツプロバイダ101と間の相互認証で得られたセッション鍵データK<sub>SES</sub>を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0102】＜決算処理＞次に、EMDサービスセンタ102において行なう決済処理について説明する。EMDサービスセンタ102は、ユーザホームネットワーク103の例えばSAM1051から利用履歴データ108およびその署名データS<sub>IG200,SAM1</sub>を入力すると、利用履歴データ108および署名データS<sub>IG200,SAM1</sub>を、SAM1051と間の相互認証によって得られたセッション鍵データK<sub>SES</sub>を用いて復号し、SAM1051の公開鍵データK<sub>SAM1</sub>による署名データS<sub>IG200,SAM1</sub>の検証を行う。

【0103】図21は、利用履歴データ108に記述されるデータを説明するための図である。図21に示すように、利用履歴データ108には、例えば、セキヤコンテナ104に格納されたコンテンツデータCに対してEMDサービスセンタ102によってグローバルユニークに付された識別子であるESC\_コンテンツID、当該コンテンツデータCに対してコンテンツプロバイダ101によって付された識別子であるCP\_コンテンツID、セキヤコンテナ104の配給を受けたユーザの識

別子であるユーザID、当該ユーザのユーザ情報、セキュアコンテナ104の配給を受けたSAM105<sub>1</sub>～105<sub>4</sub>の識別子SAM\_ID、当該SAMが属するホームネットワークグループの識別子であるHNG\_ID、ディスクカウント情報、トレーシング情報、プライスタグ、当該コンテンツデータを提供したコンテンツプロバイダ101の識別子CP\_ID、紹介業者（ポータル:Portal）ID、ハードウェア提供者ID、セキュアコンテナ104を記録した記録媒体の識別子Media\_ID、セキュアコンテナ104の用に用いられた例えば圧縮方法などの所定のコンポーネントの識別子であるコンポーネントID、セキュアコンテナ104のライセンス所有者の識別子LH\_ID、セキュアコンテナ104についての決済処理を行うEMDサービスセンタ102の識別子ESC\_IDなどが記述されている。なお、後述する第2実施形態では、利用履歴データ308には、上述した利用履歴データ108に記述されたデータに加えて、当該コンテンツデータCに対してサービズプロバイダ310によって付された識別子であるSP\_IDと、当該コンテンツデータCを配給したサービズプロバイダ310の識別子SP\_IDとが記述されている。

【0104】EMDサービスセンタ102は、コンテンツプロバイダ101の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク103のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ107および決済請求権データ152を作成する。当該分配率表は、例えば、セキュアコンテナ104に格納されたコンテンツデータ毎に作成される。

【0105】次に、EMDサービスセンタ102は、利用履歴データ108と、権利書データベースから読み出した権利書データ106に含まれる標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を生成する。ここで、決済請求権データ152は、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

【0106】次に、EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG99を、相互認証およびセッション鍵データK<sub>SES</sub>による符号を行なった後に、図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。これにより、決済請求権データ152に示される金額の金銭が、コンテンツプロバイダ101に支払われる。また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0107】ユーザホームネットワーク103は、図1に示すように、ネットワーク機器160<sub>1</sub>およびA/V機器160<sub>2</sub>～160<sub>4</sub>を有している。ネットワーク機器160<sub>1</sub>は、SAM105<sub>1</sub>を内蔵している。また、A/V機器160<sub>2</sub>～160<sub>4</sub>は、それぞれSAM105<sub>2</sub>～105<sub>4</sub>を内蔵している。SAM105<sub>1</sub>～105<sub>4</sub>の相互間は、例えば、IEEE1394シリアルインタフェースバスなどのバス191を介して接続されている。なお、A/V機器160<sub>2</sub>～160<sub>4</sub>は、それぞれネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器160<sub>1</sub>のネットワーク通信機能を利用していてもよい。また、ユーザホームネットワーク103は、ネットワーク機能を有していないA/V機器のみを有していてもよい。

【0108】以下、ネットワーク機器160<sub>1</sub>について説明する。図22は、ネットワーク機器160<sub>1</sub>の構成図である。図22に示すように、ネットワーク機器160<sub>1</sub>は、SAM105<sub>1</sub>、通信モジュール162、AV圧縮・伸長用SAM163、操作部165、ダウンロードメモリ167、再生モジュール169、外部メモリ201およびホストCPU810を有する。ここで、ホストCPU810はネットワーク機器160<sub>1</sub>内の処理を統括的に制御しており、ホストCPU810とSAM105<sub>1</sub>とは、それぞれマスター(Master)とスレーブ(Slave)の関係にある。以下、ホストCPU810とSAM105<sub>1</sub>との関係を詳細に説明する。図23は、ホストCPU810とSAM105<sub>1</sub>との関係を説明するための図である。図23に示すように、ネットワーク機器160<sub>1</sub>では、ホストCPUバス1000を介して、ホストCPU810とSAM105<sub>1</sub>とが接続されている。ホストCPU810は、例えばユーザによる操作部165の操作に応じて複数の割り込みタイプの中から割り込みタイプが選択された場合に、当該選択された割り込みタイプを示す外部割り込み（ハードウェア割り込み）S165を受ける。また、ホストCPU810は、外部割り込みS165を受け、当該外部割り込みS165に対応するタスクがSAM105<sub>1</sub>が実行すべきものである場合に、当該タスクを指定した内部割り込み（ソフトウェア割り込み）S810を、ホストCPUバス1000を介してSAM105<sub>1</sub>に出す。

【0109】SAM105<sub>1</sub>は、ホストCPU810から1/Oデバイスとして認識され、ホストCPU810からのファンクションコールである内部割り込みS810を受けて、要求に応じたタスクを実行し、当該タスクの実行結果をホストCPU810に返す。SAM105<sub>1</sub>が実行するタスクは、主に、コンテンツデータの購入処理（購金処理）、署名検証処理、相互認証処理、コンテンツデータの再生処理、更新処理、登録処理、ダウンロード処理などに関するものであり、これらのタスク群



はSAM105<sub>1</sub>内で外部から遮蔽された形で処理され、ホストCPU810は当該処理内容をモニタできない。ホストCPU810は、どのようなイベントのときにSAM105<sub>1</sub>にタスクを依頼するかを予め把握している。具体的には、ホストCPU810は、ユーザによる外部キーデバイスなどの操作部165の操作に応じた外部割り込みS165を受けて、当該割り込みによって実行すべきタスクがSAM105<sub>1</sub>が実行するタスクであると判断すると、ホストCPUバス1000を介してSAM105<sub>1</sub>に内部割り込みS810をかけ、SAM105<sub>1</sub>に当該タスクを実行させる。

【0110】ここで、コマンダーおよびキーボードなどの外部キーデバイスなどのホストCPU810に対してのI/Oデバイスに相当するものから受ける割り込みは、ホストCPU810が実行するユーザプログラムの内容とは全く非同期的なイベントによって生じる割り込みであり、通常、これらを“ハードウェア割り込み”あるいは“外部割り込み”と呼んでいる。ホストCPU810が、コンテンツの視聴および購入時に受ける割り込みは、ハードウェア割り込みである。このとき、ハードウェア割り込みを発生するI/Oデバイスは、例えば、ネットワーク機器160<sub>1</sub>のボタン類やGUI(Graphical User Interface)のアイコンなどのキーデバイスである。本実施形態では、これらのI/Oデバイスを操作部165としている。

【0111】一方、ホストCPU810によるユーザプログラム(プログラム)の実行に基づいて発生する割り込みは、“ソフトウェア割り込み”または“内部割り込み”と呼ばれる。

【0112】外部割り込みS165は、通常、その割り込み信号を、ホストCPUバス1000とは別に設けられた外部割り込み専用線を介して操作部165からホストCPU810に出力している。外部割り込みS165の種類は、割り込みが発生するI/Oデバイスに番号を持たせることで区別される。例えば、キーボードなどでは、全てのボタン(当該番号を割り込みタイプと呼ぶ)に番号が割り当てられ、ボタンが押されると、当該ボタンが押下されたことを外部割り込み専用線を介して操作部165からホストCPU810に通知し、当該押下されたボタンの番号をI/Oインターフェイス内のメモリに記憶する。そして、ホストCPU810は、ボタンが押下されたことの通知を受けると、I/Oインターフェイス内のメモリにアクセスを行い、当該メモリに記憶されたボタンの番号から外部割り込みのタイプを識別し、当該ボタンの番号に対応する割り込みルーチンの実行制御を行う。このとき、ホストCPU810が、当該ボタンの番号に対応する割り込みルーチンがSAM105<sub>1</sub>によって実行されるべきものである場合には、SAM105<sub>1</sub>に内部割り込みS810を出してタスク実行を依頼する。

【0113】前述したように、SAM105<sub>1</sub>が実行するタスクには、以下に示す①～③などがある。これらのタスクは、外部割り込み専用線を介してホストCPU810が①～③などに対応する外部割り込みを操作部165から受け、ホストCPU810がそれに応じた内部割り込みS810をSAM105<sub>1</sub>に出すことで、SAM105<sub>1</sub>によって実行される。

- ①. コンテンツ購入処理(鍵の購入処理。試験含む。)
- ②. 再生処理
- ③. コンテンツプロバイダ101およびEMDサービスセンタ102からのダウンロード(更新処理、利用履歴回収、プログラムダウンロードなど)

【0114】上記①、②では、割り込みを発生させるI/Oはネットワーク機器160<sub>1</sub>のボタンやGUIなどの外部キーデバイスになる。上記③は、実際は、コンテンツプロバイダ101からブッシュ的にダウンロード用のセキュアコンテナ104が送られてくるのではなく、ネットワーク機器160<sub>1</sub>(クライアント)側からボーリングしにいて能動的プル型のため、ダウンロードしたセキュアコンテナ104をネットワーク機器160<sub>1</sub>内のダウンロードメモリ167に書き込んだ時点で、その状態をホストCPU810は把握している。従って、上記③の場合には、ホストCPU810は、操作部165からの外部割り込みS165を受けることなく、SAM105<sub>1</sub>に対して内部割り込みS810を発生する。

【0115】SAM105<sub>1</sub>は、ホストCPU810に対してスレープのI/Oデバイスと機能するので、SAM105<sub>1</sub>のメインルーチンは電源オンでスタートしてから、その後はスタンバイ(ウェーティング、待ち状態)モードで待機している。その後、SAM105<sub>1</sub>は、マスタであるホストCPU810から内部割り込みS810を受けた時点で、内部で外部から遮蔽された形で依頼されたタスクを処理し、タスク終了をホストCPU810に外部割り込み(ハードウェア割り込み)で知らせ、ホストCPU810に当該そのタスク結果を返してもらう。従って、SAM105<sub>1</sub>には、ユーザのメインプログラム(ユーザプログラム)というものがない。

【0116】SAM105<sub>1</sub>は、コンテンツの購入処理、再生処理、コンテンツプロバイダ101、並びにEMDサービスセンタ102からのダウンロード処理などを割り込みルーチンとして実行する。SAM105<sub>1</sub>は、通常は、スタンバイ状態で待機している状態から、ホストCPU810から内部割り込みS810を受け、その割り込みタイプ(番号)(ファンクションコールのコード)に応じた割り込みルーチンを実行し、結果を得た時点で、それをホストCPU810に返してもらう。具体的には、ホストCPU810からSAM105<sub>1</sub>への内部割り込みS810によるタスク依頼は、I/O命令で行われ、SAM105<sub>1</sub>はホストCPU810

0から受け取ったファンクションコールのコマンドに基づいて自分自身に内部割り込みをかける。ホストCPU810によってSAM105<sub>1</sub>への内部割り込みは、具体的には、チップセレクト(Chip Select)を行ってSAM105<sub>1</sub>を選択して行われる。

【0117】上述したように、コンテンツの購入および再生などの外部割り込みS165をホストCPU810が受けるにも係わらず、それに応じたタスクをSAM105<sub>1</sub>に依頼して行うのは、それらのタスク内容が鍵の購入処理などに伴う暗号処理、署名生成、署名検証処理などのセキュリティに係わるものだからである。SAM105<sub>1</sub>に格納されている割り込みルーチンは、ホストCPU810の割り込みルーチンのサブルーチ的な役割をもつ割り込みルーチンといえる。ホストCPU810によって実行される割り込みルーチンは、SAM105<sub>1</sub>の共有メモリ空間に、自らに対して行われた外部割り込みS165に対応するタスクを依頼する内部割り込み(ファンクションコール)S810を送ることを指示するタスクである。なお、図24に示すように、SAM105<sub>1</sub>に格納されている割り込みルーチンには、さらにサブルーチンがぶらさがっている。他の割り込みルーチンに共通なプログラムは、サブルーチンとして定義したほうがコードサイズの節約になり、メモリの削減になるためである。また、SAM105<sub>1</sub>の処理は、割り込みルーチンから並列にサブルーチンを定義したり、サブルーチンのさらにサブルーチンを定義するなど、通常のCPUの処理と同様の手法が採用されている。

【0118】図23に戻って説明を行う。前述したように、ホストCPU810は、外部キーデバイスなどのI/Oからの割り込みを、割り込み専用線による外部割り込み(ハードウェア割り込み)S165として受ける。各々の外部割り込み専用線には、番号が割り振られていて、その番号に応じてホストCPU810側のシステムメモリに格納されている割り込みベクタテーブルにおいて、相当の割り込みベクタを抜き出して割り込みルーチンを開始する。そのとき、割り込みタイプが、ベクタテーブルの中の割り込みベクタの選択番号を示す間接アクセス、割り込みタイプが、そのまま割り込みルーチンの開始アドレスを示す直接アクセスの2種類が存在する。

【0119】ホストCPU810は、受けた外部割り込みが、SAM105<sub>1</sub>が行うべきタスクの場合、割り込みルーチンは、SAM105<sub>1</sub>に対して内部割り込みS810をかけ、SAM105<sub>1</sub>にタスクを実行するように依頼(I/O命令)するプログラムである。タスクの種類はコマンド名で定義されていて、ホストCPU810はSAM105<sub>1</sub>に対してコマンドベースの内部割り込みS810をかける。SAM105<sub>1</sub>は電源オンしたとき、図24に示すように、初期化プログラムとSAM内部のIntegrity Checkを済ませ、その後はスタンバイ

状態で待機するスリープモードとなる。スリープモードでは、CPUの動作のみを停止させ、すべての割り込みで復帰する。その後、SAM105<sub>1</sub>は、例外処理状態を経てプログラム実行状態に移転する。その後は、SAM105<sub>1</sub>は、ホストCPU810からのタスク依頼の内部割り込みを受けた時点で相当のタスクを実行して結果を出し、それをホストCPU810に返す。ホストCPU810は、その結果を受けて次のアクションを行う。但し、SAM105<sub>1</sub>がタスク実行中でも、ホストCPU810は他のタスクを行ってもよい。ホストCPU810は、SAM105<sub>1</sub>によるタスクの実行結果を割り込みとして受けつける。

【0120】SAM105<sub>1</sub>が、ホストCPU810から依頼を受けたタスクの実行結果をホストCPU810に知らせる手段としては、ホストCPU810に対し割り込みをかけて、ホストCPU810に当該実行結果を拾ってもらう方法と、SAM105<sub>1</sub>の内部のホストCPU810がアクセス可能なアドレス空間上(当該アドレス空間には、ホストCPU810からのリード/ライトコマンド、アドレス情報、データがキャリアされる)にステータスレジスタ(SAMステータスレジスタと呼ぶ)を設ける方法とがある。後者の方法では、SAMステータスレジスタ(SAM-SR)にタスクの種類、タスク待機中、タスク実行中、タスク終了などのフラグを設定できるように、当該SAMステータスレジスタに、ホストCPU810から定期的にポーリング(データの読み込み)を行う。

【0121】第1のSAMステータスレジスタには、ホストCPU810によって読み出される、SAM105<sub>1</sub>のステータス(状態)を示すフラグが設定される。また、第2のSAMステータスレジスタには、ホストCPU810からタスク実行の依頼が出されているか否かのステータスをSAM105<sub>1</sub>の内部のCPUから読み込むフラグが設定される。バス制御の優先順位に基づいて、ホストCPU810とSAM105<sub>1</sub>との双方が、当該第1および第2のSAMステータスレジスタのフラグにアクセスできる。

【0122】具体的に、第1のSAMステータスレジスタには、現在SAMがタスクを実行中か否か、タスク終了済で結果が得られているか否か、そのときのタスク名は何か、あるいはSAMは現在スタンバイ中でタスク待ちの状態か否かを示すフラグが設けられている。第1のSAMステータスレジスタには、ホストCPU810が定期的にポーリングしにいく。一方、第2のSAMステータスレジスタには、ホストCPU810からタスク実行の依頼が発生しているか否か、あるいは待機中か否かを示すフラグが設けられている。ここで、ホストCPU810からは、I/O書き込み命令のコマンドがI/OデバイスであるSAM105<sub>1</sub>に送られ、続いて、書き込むデータと書き込むアドレス情報が送られる。その

ときのアドレス情報（データの格納場所）はホストCPU 810とSAM1051との共有メモリ空間内に格納される。

【0123】ここで、SAM1051内のメモリのアドレス空間は、ホストCPU 810側からは見えないようにすることが必要なので（耐タンパ性）、ホストCPU 810からは、作業スタック用のSRAMの一部、あるいは外付けのFlash-ROM（EEPROM）の一部しか見えないように、SAM1051内のアドレス空間を管理する回路を構成する。従って、ホストCPU 810から、データ量の大きいものは、これらのエリアにデータを書き込んでいくし、データ量の少ないものはSAM1051の内部に、ホストCPU 810から見えるように仮設のレジスタを設定して、そこに書き込む。

【0124】割り込みによって実行される割り込みルーチンのアドレスは「割り込みベクタ」と呼ばれる。割り込みベクタは、割り込みタイプの順に割り込みベクタテーブルに格納されている。

【0125】ホストCPU 810は、図25に示すように、外部割り込みを受けると、その割り込みタイプ（番号）にしたがって、メモリに格納された割り込みベクタテーブルから割り込みベクタを取り出し、そのアドレスから始まるルーチンをサブルーチンとして実行する。本実施形態では、前述した①～③の場合に、対応するI/Oから物理的な割り込み信号によって外部割り込みが発生し、その割り込みタイプ（番号）にしたがって実行される割り込みルーチンで、I/OであるSAM1051に対して内部割り込み（ソフトウェア割り込み）を利用したファンクションコール（Procedure Call）を行い、自分の代わりにSAM1051にそのタスクの実行を行ってもらい、その結果を受け取って次なるアクションを行う。内部割り込みは、図26に示すように、ユーザプログラム中、つまりCPU内部から発生するソフトウェア割り込みである。当該内部割り込みは、マシン語のINT命令の実行によって発生する。

【0126】以下、ファンクションコール（Procedure Call）について説明する。割り込みルーチンの中は、さらに細かく機能（ファンクション）に分けられていて、各機能にコマンド名が定義されている。ここで、ユーザプログラムから、割り込み命令INTと共にコマンドを指定することで、目的の機能を指定することをファンクションコール（Procedure Call）とよぶ。ファンクションコールは、内部割り込み（ソフトウェア割り込み）を利用したものである。ファンクションコールでは、CPUのレジスタにファンクションコール番号を入れて割り込みルーチンに必要なパラメータを渡し、目的の機能（ファンクション）を指定する。その結果はレジスタやメモリに返されるか、あるいは動作が完了してあらわれる。例えば、ホストCPU 810が図27に示すユーザプログラム内のコードAを実行する場合に、「INT

21H」によってCPUによって割り込みタイプ「21H」の内部割り込みに対応するメモリ内の領域がアクセスされ、コマンド解析部へのアクセスを介して、ファンクション3のサブルーチンが実行される。

【0127】次に、SAM1051のCPUの処理状態について説明する。図28は、SAM1051のCPUの処理状態を説明するための図である。図28に示すように、SAM1051のCPUの処理状態には、リセット状態ST1、例外処理状態ST2、バス権解放状態ST3、プログラム実行状態ST4および低消費電力状態ST5の5種類がある。以下、各状態について説明する。

リセット状態ST1：CPUがリセットされている状態である。

例外処理状態ST2：リセットや割り込みなどの例外処理要因によってCPUが処理状態の流れを変えるときに過渡的な状態である。割り込みの処理の場合は、SP（スタックポインタ）を参照してPC（プログラムカウンタ）のカウント値とステータスレジスタ（SR）の値とをスタック領域に退避する。例外処理ベクタテーブルから割り込みルーチンの開始アドレスを取り出し、そのアドレスに分歧してプログラムの実行を開始する。その後の処理状態はプログラム実行状態ST3となる。

【0128】プログラム実行状態ST3：CPUが順次プログラムを実行している状態である。バス権解放状態ST4：CPUがバス権を要求したデバイスにバスを解放する状態である。

【0129】低消費電力状態ST5：スリープモード、スタンバイモードおよびモジュールスタンバイモードの3つの状態がある。

#### （1）スリープモード

CPUの動作は停止するが、CPUの内部レジスタのデータと、内蔵キャッシュメモリ、および内蔵RAMのデータは保持される。CPU以外の内蔵周辺モジュールの機能は停止しない。このモードからの復帰は、リセット、すべての割り込み、またはDMAアドレスエラーによって行われ、例外処理状態ST2を経て通常のプログラム実行状態へ遷移する。

#### （2）スタンバイモード

スタンバイモードでは、CPU、内蔵モジュール、および発振器のすべての機能が停止する。キャッシュおよび内部RAMのデータは保持されない。スタンバイモードからの復帰は、リセット、外部のNMI割り込みにより行われる。復帰時は、発振安定時間経過後、例外処理状態を経て通常プログラム状態へ遷移する。発振器が停止するので、消費電力は著しく低下する。

#### （3）モジュールスタンバイモード

DMAなどの内蔵モジュールへのクロック供給を停止することができる。

【0130】次に、ホストCPU 810とSAM1051

1 との間の関係をメモリ空間を用いて説明する。図29は、ホストCPU810およびSAM105<sub>1</sub>のメモリ空間を示す図である。図29に示すように、ホストCPU810のCPU810aは、ユーザのボタン操作などに応じた外部割り込みを受けると、ユーザプログラムの実行を中断して、割り込みタイプを指定して割り込みベクタテーブルのハードウェア割り込みの領域にアクセスする。そして、CPU810aは、当該アクセスによって得られたアドレスに記憶されている割り込みルーチンを実行する。当該割り込みルーチンは、SAMに対して内部割り込みであるファンクションコールCall11-1, 1-2, 2または3を出してSAMに対応するタスクを実行させ、そのタスク実行の結果を得た後に、ユーザプログラムに復帰する処理を記述している。具体的には、CPU8110aは、SAM105<sub>1</sub>内のメモリ105<sub>1</sub>aの一部を構成するSRAM1155に、依頼するタスクを特定する情報を書き込む。ここで、SRAM1155は、ホストCPU810とSAM105<sub>1</sub>との共有メモリである。

【0131】ホストCPU810のCPU810aは、SAM105<sub>1</sub>に内部割り込みを出すときに、SAM105<sub>1</sub>内の第2のSAMステータスレジスタ1156bのタスク待機中のフラグをオンにする。SAM105<sub>1</sub>のCPU1100は、第2のSAMステータスレジスタ1156bを見ると、SRAM1155にアクセスして依頼されたタスクの種類を特定し、それに応じた割り込みルーチンを実行する。当該割り込みルーチンは、前述したように、他のサブルーチンを読み出して実行される。当該サブルーチンには、例えば、記録媒体との相互認証、A/V圧縮・伸長用SAMとの相互認証、メディア・ドライブSAMとの間の相互認証、ICカードとの間の相互認証、機器間の相互認証、EMDサービスセンタ102との間の相互認証、並びに署名データの生成および検証を行うものがある。

【0132】SAM105<sub>1</sub>のCPU1100は、当該割り込みルーチンの結果（タスク結果）を、SRAM1155内に格納すると共に、SAM105<sub>1</sub>内の第1のSAMステータスレジスタ1156aのタスク終了のフラグをオンにする。そして、ホストCPU810は、第1のSAMステータスレジスタ1156aのタスク終了のフラグがオンにされたことを確認した後に、SRAM1155に格納されたタスク結果を読み出し、その後、ユーザプログラムの処理に復帰する。

【0133】以下、SAM105<sub>1</sub>の機能を説明する。ここで、SAM105<sub>2</sub>～105<sub>4</sub>の機能は、SAM105<sub>1</sub>の機能と同じである。SAM105<sub>1</sub>は、コンテンツ単位の課金処理を行うモジュールであり、EMDサービスセンタ102との間で通信を行う。SAM105<sub>1</sub>は、例えば、EMDサービスセンタ102によって仕様およびバージョンなどが管理され、家庭機器メーカに

対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカは、SAM105<sub>1</sub>のIC(Integrated Circuit)の内部の仕様を知ることができる。EMDサービスセンタ102が当該ICのインタフェースなどを統一化し、それに従ってネットワーク機器160<sub>1</sub>に搭載される。なお、SAM105<sub>2</sub>～105<sub>4</sub>は、それぞれAV機器160<sub>2</sub>～160<sub>4</sub>に搭載される。

【0134】SAM105<sub>1</sub>は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能なタンパ（Tamper Resistance）性を持ったハードウェアモジュール（ICモジュールなど）、あるいはCPUにおいてソフトウェア（秘密プログラム）を実行して実現される機能モジュールである。SAM105<sub>1</sub>の機能はICという形で表現する場合は、IC内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAMをICという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をSAMとして定義してもよい。

【0135】なお、図22に示す例では、実線で示されるように、通信モジュール162からのセキュアコンテンツ104をSAM105<sub>1</sub>に出力する場合を示しているが、点線で示されるように、通信モジュール162からSAM105<sub>1</sub>にキーファイルKFを出力し、通信モジュール162からダウンロードメモリ167にCPUバスなどを介してコンテンツファイルCFを直接的にダウンロードメモリ167に書き込むようにしてもよい。また、AV圧縮・伸長用SAM163に対してのコンテンツデータCの出力は、SAM105<sub>1</sub>を介して行うのではなく、ダウンロードメモリ167から直接的に行うようにしてもよい。

【0136】以下、SAM105<sub>1</sub>の機能を機能ブロック図を参照しながら具体的に説明する。図30は、SAM105<sub>1</sub>の機能の機能ブロック図である。なお、図30には、コンテンツプロバイダ101からのセキュアコンテンツ104を入力し、セキュアコンテンツ104内のキーファイルKFを復号する処理に関連するデータの流れが示されている。図30に示すように、SAM105<sub>1</sub>は、相互認証部170、暗号化・復号部171、172、173、コンテンツプロバイダ管理部180、ダウンロードメモリ管理部182、AV圧縮・伸長用SAM管理部184、EMDサービスセンタ管理部185、利用監視部186、課金処理部187、署名処理部189、SAM管理部190、メディアSAM管理部197、作業用メモリ200、外部メモリ管理部811およびCPU1100を有する。CPU1100は、ホストCPU810からの内部割り込みS810を受けて、S

AM105<sub>1</sub> 内の処理を統括的に制御する。

【0137】ここで、コンテンツプロバイダ管理部180およびダウンロードメモリ管理部182が本発明の入力処理手段に対応し、課金処理部187が本発明の決定手段、履歴データ生成手段および利用制御データ生成手段に対応し、暗号化・復号部172が本発明の復号手段に対応し、利用監視部186が本発明の利用制御手段に対応している。また、暗号化・復号部173が本発明の暗号化手段に対応している。また、後述する例えば図45に示すメディア・ドライブSAM管理部855が本発明の記録制御手段に対応している。また、署名処理部189が本発明の署名処理手段に対応している。

【0138】なお、図30に示すSAM105<sub>1</sub>の各機能は、前述したように、CPUにおいて秘密プログラムを実行して実現されるか、あるいは所定のハードウェアによって実現される。SAM105<sub>1</sub>のハードウェア構成については後述する。また、外部メモリ201には、以下に示す処理を経て、図31に示すように、利用履歴データ108およびSAM登録リストが記憶される。ここで、外部メモリ201のメモリ空間は、SAM105<sub>1</sub>の外部（例えば、ホストCPU810）からは見ることはできず、SAM105<sub>1</sub>のみが外部メモリ201の記憶領域に対してのアクセスを管理できる。外部メモリ201としては、例えば、フラッシュメモリあるいは強誘電体メモリ（FeRAM）などが用いられる。また、作業用メモリ200としては、例えばSRAMが用いられ、図32に示すように、セキュアコンテナ104、コンテンツ鍵データK<sub>c</sub>、権利書データ（UCP）106、記憶部192のロック鍵データK<sub>LOC</sub>、コンテンツプロバイダ101の公開鍵証明書CER<sub>CP</sub>、利用制御データ（UCS）166、およびSAMプログラム・ダウンロード・コンテナSDC<sub>1</sub>～SDC<sub>3</sub>などが記憶される。

【0139】以下、SAM105<sub>1</sub>の機能のうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力（ダウンロード）したときの各機能ブロックの処理内容を図30を参照しながら説明する。当該処理は、コンテンツのダウンロードを指示する外部割込みS810をホストCPU810から受けたCPU1100によって統括的に制御される。

【0140】相互認証部170は、SAM105<sub>1</sub>がコンテンツプロバイダ101およびEMDサービスセンタ102との間でオンラインでデータを送受信する際に、コンテンツプロバイダ101およびEMDサービスセンタ102との間で相互認証を行ってセッション鍵データ（共有鍵）K<sub>SES</sub>を生成し、これを暗号化・復号部171に出力する。セッション鍵データK<sub>SES</sub>は、相互認証を行う度に新たに生成される。

【0141】暗号化・復号部171は、コンテンツプロバイダ101およびEMDサービスセンタ102との間

で送受信するデータを、相互認証部170が生成したセッション鍵データK<sub>SES</sub>を用いて暗号化・復号する。

【0142】ダウンロードメモリ管理部182は、図22に示すようにダウンロードメモリ167が相互認証機能を持つメディアSAM167aを有している場合には、相互認証部170とメディアSAM167aとの間で相互認証を行った後に、相互認証によって得られたセッション鍵データK<sub>SES</sub>を用いて暗号化された図22に示すダウンロードメモリ167に書き込む。ダウンロードメモリ167としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。なお、図33に示すように、HDD（Hard Disk Drive）などの相互認証機能を備えていないメモリをダウンロードメモリ211として用いる場合には、ダウンロードメモリ211内はセキュアではないので、コンテンツファイルKFをダウンロードメモリ211にダウンロードし、機密性の高いキーファイルKFを例えば、図30に示す作業用メモリ200あるいは図22に示す外部メモリ201にダウンロードする。キーファイルKFを外部メモリ201に記憶する場合には、例えば、SAM105<sub>1</sub>において、キーファイルKFをCBCモードでMAC鍵データK<sub>MAC</sub>を用いて暗号化して外部メモリ201に記憶し、最後の暗号文ブロックの一部をMAC（Message Authentication Code）値としSAM105<sub>1</sub>内に記憶する。そして、外部メモリ201からSAM105<sub>1</sub>にキーファイルKFを読み出す場合には、SAM105<sub>1</sub>内で当該読み出したキーファイルKFをMAC鍵データK<sub>MAC</sub>を用いて復号し、それによって得たMAC値と、既に記憶しているMAC値とを比較することで、キーファイルKFが改竄されているか否かを検証する。この場合に、MAC値ではなく、ハッシュ値を用いてもよい。

【0143】暗号化・復号部172は、ダウンロードメモリ管理部182から入力したセキュアコンテナ104に格納されたキーファイルKF内のコンテンツ鍵データK<sub>c</sub>、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC<sub>1</sub>～SDC<sub>3</sub>を、記憶部192から読み出した対応する期間のライセンス鍵データKD<sub>1</sub>～KD<sub>3</sub>を用いて復号する。当該復号されたコンテンツ鍵データK<sub>c</sub>、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC<sub>1</sub>～SDC<sub>3</sub>は、作業用メモリ200に書き込まれる。

【0144】EMDサービスセンタ管理部185は、図1に示すEMDサービスセンタ102との間の通信を管理する。

【0145】署名処理部189は、記憶部192から読み出したEMDサービスセンタ102の公開鍵データK<sub>ESC</sub>およびコンテンツプロバイダ101の公開鍵データK<sub>CP</sub>を用いて、セキュアコンテナ104内の署名データの検証を行なう。

【0146】記憶部192は、SAM105<sub>1</sub>の外部か

ら読み出しおよび書き換えできない秘密データとして、図34に示すように、有効期限付きの複数のライセンス鍵データKD<sub>1</sub>～KD<sub>3</sub>、SAM\_ID、ユーザID、パスワード、当該SAMが属するホームネットワークループの識別子HNG\_ID、情報参照用ID、SAM登録リスト、機器および記録媒体のリポーションリスト、記録用鍵データKSTR、ルートCAの公開鍵データKR-CA、P、EMDサービスセンタ102の公開鍵データKESC、P、EMDサービスセンタ102の公開鍵データKESC、P、ドライブ用SAMの認証用元鍵（共通鍵暗号化方式を採用した場合）、ドライブ用SAMの公開鍵証明書（秘密鍵暗号化方式を採用した場合）、SAM1051の秘密鍵データKSAMI、S（共通鍵暗号化方式を採用した場合）、SAM1051の公開鍵データKSAMI、Pを格納した公開鍵証明書CERSAMI（秘密鍵暗号化方式を採用した場合）、EMDサービスセンタ102の秘密鍵データKESC、Sを用いた公開鍵証明書CERESCの署名データSIG<sub>22</sub>、AV圧縮・伸長用SAM163との間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアSAMとの間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアSAMの公開鍵証明書データCERMEDSAM（公開鍵暗号化方式を採用した場合）、扱える信号の諸元、圧縮方式、接続するモニタ表示能力、フォーマット変換機能、ビットストリームレコーダが有無、権利処理（利益分配）用データ、利益分配する関連エンティティのIDなどを記憶している。なお、図34において、左側に「\*」を付したデータは、SAM1051の出荷時に記憶部192に記憶されており、それ以外のデータは出荷後に行われるユーザ登録時に記憶部192に記憶される。

【0147】また、記憶部192には、図30に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。記憶部192としては、例えば、フラッシュEEPROM(Electrically Erasable Programmable RAM)が用いられる。

【0148】＜ライセンス鍵データの受信時の処理＞以下、EMDサービスセンタ102から受信したライセンス鍵データKD<sub>1</sub>～KD<sub>3</sub>を記憶部192に格納する際のSAM1051内での処理の流れを図33および図35を参照しながら説明する。図35は、EMDサービスセンタ102から受信したライセンス鍵データKD<sub>1</sub>～KD<sub>3</sub>を記憶部192に格納する際のSAM1051内での処理の流れを示すフローチャートである。ステップS35-0：SAM1051のCPU1100は、ホストCPU810から、ライセンス鍵データの受信処理を行うことを指示する内部割り込みS810を受ける。ステップS35-1：SAM1051の相互認証部170と、EMDサービスセンタ102との間で相互認証を行なう。

ステップS35-2：ステップS35-1の相互認証によって得られたセッション鍵データK<sub>SES</sub>で暗号化した3カ月分のライセンス鍵データKD<sub>1</sub>～KD<sub>3</sub>およびその署名データSIG<sub>KD1</sub>、ESC～SIG<sub>KD3</sub>、ESCを、EMDサービスセンタ102からEMDサービスセンタ管理部185を介して作業用メモリ200に書き込む。

【0149】ステップS35-3：暗号化・復号部171は、セッション鍵データK<sub>SES</sub>を用いて、ライセンス鍵データKD<sub>1</sub>～KD<sub>3</sub>およびその署名データSIG<sub>KD1</sub>、ESC～SIG<sub>KD3</sub>、ESCを復号する。

ステップS35-4：署名処理部189は、作業用メモリ200に記憶された署名データSIG<sub>KD1</sub>、ESC～SIG<sub>KD3</sub>、ESCの正当性を確認した後、ライセンス鍵データKD<sub>1</sub>～KD<sub>3</sub>を記憶部192に書き込む。

ステップS35-5：CPU1100は、上述したライセンス鍵データ受信処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。なお、CPU1100は、上述したライセンス鍵データ受信処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0150】＜セキュアコンテナ104をコンテンツプロバイダ101から入力した時の処理＞以下、コンテンツプロバイダ101が提供したセキュアコンテナ104を入力する際のSAM1051内での処理の流れを図30および図36を参照しながら説明する。なお、以下に示す例では、コンテンツファイルCFをSAM1051を介してダウンロードメモリ167に書き込む場合を例示するが、本発明は、コンテンツファイルCFをSAM1051を介さずに直接的にダウンロードメモリ167に書き込むようにしてもよい。図36は、コンテンツプロバイダ101が提供したセキュアコンテナ104を入力する際のSAM1051内での処理の流れを示すフローチャートである。なお、以下に示す例では、SAM1051において、セキュアコンテナ104を入力したときに種々の署名データの検証を行う場合を例示するが、セキュアコンテナ104の入力したときには当該署名データの検証を行わずに、購入・利用形態を決定するときに当該署名データの検証を行うようにしてもよい。

ステップS36-0：図30に示すSAM1051のCPU1100は、ホストCPU810から、セキュアコンテナの入力処理を行うことを指示する内部割り込みS810を受ける。

ステップS36-1：SAM1051の相互認証部170とコンテンツプロバイダ101との間で相互認証を行なう。

ステップS36-2：SAM1051の相互認証部170とダウンロードメモリ167のメディアSAM167aとの間で相互認証を行なう。

【0151】ステップS36-3：コンテンツプロバイ

ダ101から受信したセキュアコンテナ104を、ダウンロードメモリ167に書き込む。このとき、ステップS36-2で得られたセッション鍵データを用いて、相互認証部170におけるセキュアコンテナ104の暗号化と、メディアSAM167aにおけるセキュアコンテナ104の復号を行なう。

ステップS36-4: SAM105<sub>1</sub>は、ステップS36-1で得られたセッション鍵データを用いて、セキュアコンテナ104の復号を行なう。

【0152】ステップS36-5: 署名処理部189は、図3(C)に示す署名データSIG<sub>1</sub>ESCの検証を行なった後に、図3(C)に示す公開鍵証明書データCERCP内に格納されたコンテンツプロバイダ101の公開鍵データKCP<sub>p</sub>を用いて、署名データSIG<sub>6</sub>CP、SIG<sub>7</sub>CPの正当性を検証する。このとき、署名データSIG<sub>6</sub>CPが正当であると検証されたときに、コンテンツファイルCFの作成者および送信者の正当性が確認される。また、署名データSIG<sub>7</sub>CPが正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

【0153】ステップS36-6: 署名処理部189は、記憶部192から読み出した公開鍵データKESC<sub>p</sub>を用いて、図3(B)に示すキーファイルKF内の署名データSIG<sub>K1</sub>ESCの正当性、すなわちキーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102に登録されているか否かの検証を行う。

【0154】ステップS36-7: 暗号化・復号部172は、記憶部192から読み出した対応する期間のライセンス鍵データKD<sub>1</sub>~KD<sub>3</sub>を用いて、図3(B)に示すキーファイルKF内のコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC<sub>1</sub>~SDC<sub>3</sub>を復号し、これらを作業用メモリ200に書き込む。

【0155】ステップS36-8: CPU1100は、上述したセキュアコンテナの入力処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。なお、CPU1100は、上述したセキュアコンテナの入力処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0156】以下、ダウンロードメモリ167にダウンロードされたコンテンツデータCを利用・購入する処理に関連する各機能ブロックの処理内容を図37を参照しながら説明する。以下に示す各機能ブロックの処理は、ホストCPU810からの内部割り込みS810を受けたCPU1100によって統括的に制御される。

【0157】利用監視部186は、作業用メモリ200から権利書データ106および利用制御データ166を読み出し、当該読み出した権利書データ106および利

用制御データ166によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。ここで、権利書データ106は、図36を用いて説明したように、復号後に作業用メモリ200に記憶されたキーファイルKF内に格納されている。また、利用制御データ166は、後述するように、ユーザによって購入形態が決定されたときに、作業用メモリ200に記憶される。なお、利用制御データ166には、当該コンテンツデータCを購入したユーザのユーザIDおよびトレーシング(tracing)情報が記述され、取扱制御情報として購入形態決定処理で決定された購入形態が記述されている点を除いて、図3に示す権利書データ106と同じデータが記述されている。

【0158】課金処理部187は、図22に示すホストCPU810からコンテンツの購入あるいは利用の形態を決定することを指示する内部割り込みS810を受けたときに、それに応じた利用履歴データ108を作成する。ここで、利用履歴データ108は、前述したように、ユーザによるセキュアコンテナ104の購入および利用の形態の履歴を記述しており、EMDサービスセンタ102において、セキュアコンテナ104の購入に応じた決済処理およびライセンス料の支払いを決定する際に用いられる。

【0159】また、課金処理部187は、必要に応じて、作業用メモリ200から読み出した販売価格あるいは標準小売価格データSRPをユーザに通知する。ここで、販売価格および標準小売価格データSRPは、復号後に作業用メモリ200に記憶された図3(B)に示すキーファイルKFの権利書データ106内に格納されている。課金処理部187による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【0160】また、課金処理部187は、外部割り込みS810に基づいて、ユーザによって決定されたコンテンツの購入形態を記述した利用制御(UCS: Usage Control Status)データ166を生成し、これを作業用メモリ200に書き込む。本実施形態では、購入形態を決定した後に、利用制御データ166を作業用メモリ200に記憶する場合を示したが、利用制御データ166およびコンテンツ鍵データKcを外付けメモリである外部メモリ201に格納するようにしてもよい。外部メモリ201としては、前述したように、例えばNVRAMであるフラッシュメモリが用いられる。外部メモリ201に書き込みを行う場合には外部メモリ201の正当性の検証であるインテグリティチェック(Integrity Check)を行うが、この際に外部メモリ201の記憶領域を複数のブロックに分け、ブロック毎にSHA-1あるいはMACなどでハッシュ値を求め、当該ハッシュ値をSAM10

5<sub>1</sub>内で管理する。なお、SAM105<sub>1</sub>において、購入形態を決定せずに、セキュアコンテンツ104を他のSAM105<sub>2</sub>～105<sub>4</sub>に転送してもよい。この場合には、利用制御データ166は作成されない。

【0161】コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切り(Sell Through)、利用期間に制限を持たせるタイムリミテッド(Time Limited)、再生する度に課金を行なう再生課金(Pay Per Play)、SCMS機器を用いた複製において再生する度に課金を行なう再生課金(Pay Per SCMS)、SCMS機器において複製を認める(Sell Through SCMSCopy)、および複製のガードを行わずに再生する度に課金を行う再生課金(Pay Per Copy Without copy guard)などがある。ここで、利用制御データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態に許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御データ166には、コンテンツのID、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれたSAMのSAM\_ID、購入を行なったユーザのUSER\_IDなどが記述されている。

【0162】なお、決定された購入形態が再生課金である場合には、例えば、SAM105<sub>1</sub>からコンテンツプロバイダ101に利用制御データ166をコンテンツデータの購入と同時にリアルタイムに送信し、コンテンツプロバイダ101がEMDサービスセンタ102に、利用履歴データ108を所定の期間内にSAM105<sub>1</sub>に取りに行くことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御データ166が、コンテンツプロバイダ101およびEMDサービスセンタ102の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御データ166をコンテンツプロバイダ101にリアルタイムに送信する。

【0163】EMDサービスセンタ管理部185は、所定の期間毎に、外部メモリ管理部811を介して外部メモリ201から読み出した利用履歴データ108をEMDサービスセンタ102に送信する。このとき、EMDサービスセンタ管理部185は、署名処理部189において、秘密鍵データKSAM<sub>1</sub>を用いて利用履歴データ108の署名データSIG200、SAM<sub>1</sub>を作成し、署名データSIG200、SAM<sub>1</sub>を利用履歴データ108と共にEMDサービスセンタ102に送信する。EMDサービスセンタ102への利用履歴データ108の送信は、例えば、EMDサービスセンタ102からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報は、例えば、外部メモリ201の記憶容量に応じて決定される。

【0164】ダウンロードメモリ管理部182は、例えば、図22に示すホストCPU810からコンテンツの再生動作を行う旨の内部割り込みS810をCPU1100が受けた場合に、ダウンロードメモリ167から読み出したコンテンツデータC、作業用メモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子通知情報データ196をAV圧縮・伸長用SAM管理部184に出力する。また、AV圧縮・伸長用SAM管理部184は、ホストCPU810からの外部割り込みS165に応じてコンテンツの試験動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びに作業用メモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ199をAV圧縮・伸長用SAM管理部184に出力する。

【0165】ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試験モード時のコンテンツの取り扱いを示している。AV圧縮・伸長用SAM163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、AV圧縮・伸長用SAM163がデータ(信号)を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データKcを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試験時の再生機能を限定したり、試験可能な期間を限定するものなどがある。

【0166】<ダウンロードしたセキュアコンテンツの購入形態決定処理>以下、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテンツ104の購入形態を決定するまでのSAM105<sub>1</sub>の処理の流れを図37および図38を参照しながら説明する。なお、以下に示す処理では、セキュアコンテンツ104の購入形態を決定する際に、セキュアコンテンツ104内の各データの署名データの検証を行わない(前述したようにセキュアコンテンツ104の受信時に署名データの検証を行う)場合を例示するが、当該購入形態を決定する際にこれらの署名データの検証を行ってもよい。図38は、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテンツ104の購入形態を決定するまでの処理の流れを示すフローチャートである。

ステップS38-0:図37に示すSAM105<sub>1</sub>のCPU1100は、ホストCPU810から、コンテンツの購入形態を決定することを指示する内部割り込みS810を受ける。

【0167】ステップS38-1:CPU1100は、ホストCPU810からの内部割り込みS810が試験モードを指定しているか否かを判断し、指定されたと判



断した場合にはステップS38-2の処理を実行し、出力されていないと判断した場合にはステップS38-5の処理を実行する。

【0168】ステップS38-2：作業用メモリ200から読み出されたコンテンツ鍵データKcおよび半開示パラメータデータ199が、図32に示すAV圧縮・伸長用SAM163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データKcおよび半開示パラメータデータ199に対してセッション鍵データKsesによる暗号化および復号が行われる。

【0169】ステップS38-3：CPU110は、ホストCPU810から試験モードを行うことを示す内部割り込みS810を受けると、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、AV圧縮・伸長用SAM管理部184を介して、図22に示すAV圧縮・伸長用SAM163に出力される。このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データKsesによる暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データKsesによる暗号化・復号とが行われる。コンテンツファイルCFは、図22に示すAV圧縮・伸長用SAM163の復号部221においてセッション鍵データKsesを用いて復号された後に、復号部222に出力される。

【0170】ステップS38-4：復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データKcを用いたコンテンツデータCの復号が半開示で行われる。次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長された後に、電子透かし情報処理部224に出力される。次に、電子透かし情報処理部224においてコンテンツデータCにユーザ電子透かし情報データ196が埋め込まれ、コンテンツデータCが再生モジュール169において再生され、コンテンツ処理部224で音響が出力される。また、電子透かし情報処理部224では、コンテンツデータCに埋め込まれている電子透かし情報が検出され、当該検出の結果に基づいて、処理の停止の有無を決定する。

【0171】ステップS38-5：ユーザが操作部165を操作して購入形態を決定すると、当該決定に応じた内部割り込みS810がホストCPU810からSAM1051に出される。

ステップS38-6：SAM1051の課金処理部187において、決定された購入形態に応じた利用履歴データ108および利用制御データ166が生成され、利用履歴データ108が外部メモリ管理部811を介して外部メモリ201に書き込まれと共に、利用制御データ

166が作業用メモリ200に書き込まれる。以後は、利用監視部186において、利用制御データ166によって許諾された範囲で、コンテンツの購入および利用が行われるように制御（監視）される。

【0172】ステップS38-7：後述する図39

(C)に示す新たなキーファイルKF<sub>1</sub>が作成され、当該作成されたキーファイルKF<sub>1</sub>がダウンロードメモリ管理部182を介してダウンロードメモリ167あるいはその他のメモリに記憶される。図39(C)に示すように、キーファイルKF<sub>1</sub>に格納された利用制御データ166はストレージ鍵データKSTRおよびメディア鍵データKMEDを用いてDESのCBCモードを利用して順に暗号化されている。ここで、記録用鍵データKSTRは、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc)機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。また、メディア鍵データKMEDは、記録媒体にユニークなデータである。

【0173】ステップS38-8：署名処理部189において、SAM1051の秘密鍵データK<sub>SAM1</sub>を用いて、キーファイルKF<sub>1</sub>のハッシュ値H<sub>K1</sub>が作成され、当該作成されたハッシュ値H<sub>K1</sub>が、キーファイルKF<sub>1</sub>と対応付けられて作業用メモリ200に書き込まれる。ハッシュ値H<sub>K1</sub>は、キーファイルKF<sub>1</sub>の作成者の正当性およびキーファイルKF<sub>1</sub>が改竄されたか否かを検証するために用いられる。なお、購入形態が決定されたコンテンツデータCを、例えば、記録媒体に記録したり、オンラインを介して送信する場合には、図39に示すように、キーファイルKF<sub>1</sub>およびハッシュ値H<sub>K1</sub>、コンテンツファイルCFおよびその署名データSIG<sub>6</sub>、CP、キーファイルKFおよびその署名データSIG<sub>7</sub>、CP、公開鍵証明書データCER<sub>cp</sub>およびその署名データSIG<sub>1</sub>、ESC、公開鍵証明書データCER<sub>SAM1</sub>およびその署名データSIG<sub>22</sub>、ESCを格納したセキュアコンテナ104pが作成される。上述したようにセキュアコンテナ104の購入形態を決定すると、利用制御データ166が生成されて作業用メモリ200に記憶されるが、SAM1051において再び同じセキュアコンテナ104について購入形態を再決定する場合には、操作信号S165に応じて作業用メモリ200に記憶されている利用制御データ166が更新される。

【0174】ステップS38-9：CPU110は、上述したコンテンツの購入形態決定処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。なお、CPU110は、上述したコンテンツの購入形態決定処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0175】<コンテンツデータの再生処理>次に、ダ

ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図40を参照しながら説明する。図40は、当該処理を示すフローチャートである。当該処理を行う前提として、前述した購入形態の決定処理によって作業用メモリ200に、利用制御データ166が格納されている。

ステップS40-0：図37に示すSAM105<sub>1</sub>のCPU1100は、ホストCPU810から、コンテンツの再生処理を行うことを指示する内部割り込みS810を受ける。

【0176】ステップS40-1：作業用メモリ200から利用監視部186に、利用制御データ166が読み出され、利用制御データ166が示す再生条件が解釈・検証され、その結果に基づいて以後の再生処理が行われるように監視される。

ステップS40-2：図37に示す相互認証部170と、図22に示すAV圧縮・伸長用SAM163の相互認証部220との間で相互に認証が行われ、セッション鍵データK<sub>SES</sub>が共有される。

【0177】ステップS40-3：ステップS40-1で解釈・検証された再生条件と、作業用メモリ200から読み出されたコンテンツ鍵データK<sub>c</sub>とが、ステップS40-2で得られたセッション鍵データK<sub>SES</sub>を用いて暗号化された後に、AV圧縮・伸長用SAM163に出力される。これによって、図22に示すAV圧縮・伸長用SAM163の復号部221においてセッション鍵データK<sub>SES</sub>を用いて再生条件およびコンテンツ鍵データK<sub>c</sub>が復号される。

【0178】ステップS40-4：ダウンロードメモリ167から読み出されたコンテンツファイルCFが、ステップS40-2で得られたセッション鍵データK<sub>SES</sub>を用いて暗号化された後に、AV圧縮・伸長用SAM163に出力される。これによって、図22に示すAV圧縮・伸長用SAM163の復号部221においてセッション鍵データK<sub>SES</sub>を用いてコンテンツファイルCFが復号される。続いて、AV圧縮・伸長用SAM163の伸長部223において、コンテンツファイルCF内のコンテンツデータCが伸長され、電子透かし情報処理部224においてユーザ電子透かし情報を埋め込んだ後に再生モジュール169において再生される。

【0179】ステップS40-5：必要に応じて、ステップS40-1で読み出された利用制御データ166が更新され、再び作業用メモリ200に書き込まれる。また、外部メモリ201に記憶されている利用履歴データ108が更新あるいは作成される。

【0180】ステップS40-6：CPU1100は、上述したコンテンツの再生処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。なお、CPU1100は、上述したコンテンツの再生処理

が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0181】<一の機器の利用制御データ(USC)166を使用して他の機器で再購入を行う場合の処理>先ず、図41に示すように、例えば、ネットワーク機器160<sub>1</sub>のダウンロードメモリ167にダウンロードされたコンテンツファイルCFの購入形態を前述したように決定した後に、当該コンテンツファイルCFを格納した新たなセキュアコンテナ104<sub>x</sub>を生成し、バス191を介して、AV機器160<sub>2</sub>のSAM105<sub>2</sub>にセキュアコンテナ104<sub>x</sub>を転送するまでのSAM105<sub>1</sub>内での処理の流れを図42および図43を参照しながら説明する。

【0182】図43は、当該処理のフローチャートである。図43に示す処理を行う前提として、前述した購入処理によって、SAM105<sub>1</sub>の作業用メモリ200には図44(C)に示すキーファイルKF<sub>1</sub>およびハッシュ値H<sub>K1</sub>が記憶されている。

ステップS43-1：ユーザによる操作部165の操作に応じて、購入形態が既に決定したセキュアコンテナをSAM105<sub>2</sub>に転送することを示す内部割り込みS810を、図42に示すCPU1100が受ける。それに応じて、課金処理部187は、外部メモリ201に記憶されている利用履歴データ108を更新する。

【0183】ステップS43-2：SAM105<sub>1</sub>は、後述するSAM登録リストを検証し、セキュアコンテナの転送先のSAM105<sub>2</sub>が正規に登録されているSAMであるか否かを検証し、正規に登録されていると判断した場合にステップS43-3以降の処理を行う。また、SAM105<sub>1</sub>は、SAM105<sub>2</sub>がホームネットワーク内のSAMであるか否かの検証も行う。

【0184】ステップS43-3：相互認証部170は、SAM105<sub>2</sub>との間で相互認証を行って得たセッション鍵データK<sub>SES</sub>を共用する。

【0185】ステップS43-4：SAM管理部190は、ダウンロードメモリ211から図39(A)に示すコンテンツファイルCFおよび署名データSIG<sub>6</sub>,cpを読み出し、これについてのSAM105<sub>1</sub>の秘密鍵データK<sub>SAM1</sub>を用いた署名データSIG<sub>41</sub>,SAM<sub>1</sub>を署名処理部189に作成させる。

【0186】ステップS43-5：SAM管理部190は、ダウンロードメモリ211から図39(B)に示すキーファイルKFおよび署名データSIG<sub>7</sub>,cpを読み出し、これについてのSAM105<sub>1</sub>の秘密鍵データK<sub>SAM1</sub>を用いた署名データSIG<sub>42</sub>,SAM<sub>1</sub>を署名処理部189に作成させる。

【0187】ステップS43-6：SAM管理部190は、図44に示すセキュアコンテナ104<sub>x</sub>を作成する。

ステップS43-7:暗号化・復号部171において、ステップS43-3で得たセッション鍵データKSESを用いて、図44に示すセキュアコンテナ104xが暗号化される。

【0188】ステップS43-8: SAM管理部190は、セキュアコンテナ104xを図41に示すAV機器1602のSAM1052に出力する。このとき、SAM1051とSAM1052との間の相互認証と並行して、IEEE1394シリアルバスであるバス191の相互認証が行われる。

【0189】ステップS43-9: CPU1100は、上述した購入形態を既に決定したセキュアコンテナをSAM1052に転送する処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。なお、CPU1100は、上述した購入形態を既に決定したセキュアコンテナをSAM1052に転送する処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0190】以下、図41に示すように、SAM1051から入力した図44に示すセキュアコンテナ104xを、RAM型などの記録媒体(メディア)1304に書き込む際のSAM1052内での処理の流れを図45、図46および図47を参照して説明する。図46および図47は、当該処理を示すフローチャートである。ここで、RAM型の記録媒体1304は、例えば、セキュアでないRAM領域134、メディアSAM133およびセキュアRAM領域132を有している。

ステップS46-0: 図45に示すCPU1100は、図41に示すAV機器1602のホストCPU810から、ネットワーク機器1601からのセキュアコンテナを入力することを示す内部割り込みS810を受ける。

【0191】ステップS46-1: SAM1052は、SAM登録リストを検証し、セキュアコンテナの転送元のSAM1051が正規に登録されているSAMであるか否かを検証し、正規に登録されていると判断した場合にステップS46-2以降の処理を行う。また、SAM1052は、SAM1051がホームネットワーク内のSAMであるか否かの検証も行う。

【0192】ステップS46-2: 前述したステップS43-2に対応する処理として、SAM1052は、SAM1051との間で相互認証を行って得たセッション鍵データKSESを共用する。

ステップS46-3: SAM1052のSAM管理部190は、図41および図45に示すように、ネットワーク機器1601のSAM1051からセキュアコンテナ104xを入力する。

ステップS46-4: 暗号化・復号部171は、ステップS46-2で共用したセッション鍵データKSESを用いて、SAM管理部190を介して入力したセキュア

コンテナ104xを復号する。

【0193】ステップS46-5: セッション鍵データKSESを用いて復号されたセキュアコンテナ104x内のコンテンツファイルCFが、図43に示すメディア・ドラブSAM260におけるセクタライズ(Sectorize)、セクタヘッダの付加処理、スクランブル処理、ECCエンコード処理、変調処理および同期処理を経て、RAM型の記録媒体1304のRAM領域134に記録される。

【0194】ステップS46-6: セッション鍵データKSESを用いて復号されたセキュアコンテナ104x内の署名データSIG6, CP, SIG41, SAM1と、キーファイルKFおよびその署名データSIG7, CP, SIG42, SAM1と、キーファイルKFおよびそのハッシュ値HK1と、公開鍵署名データCERCPおよびその署名データSIG1, ESCと、公開鍵署名データCERSAM1およびその署名データSIG22, ESCとが、作業用メモリ200に書き込まれる。

【0195】ステップS46-7: 署名処理部189において、記憶部192から読み出した公開鍵データKCP, pを用いて、公開鍵証明書データCERCP, CERSAM1の正当性が確認される。そして、署名処理部189において、公開鍵証明書データCERSAM1に格納された公開鍵データKCP, pを用いて、署名データSIG6, CPの正当性が検証され、コンテンツファイルCFの作成者の正当性が確認される。また、署名処理部189において、公開鍵証明書データCERSAM1に格納された公開鍵データKSAM1, pを用いて、署名データSIG41, SAM1の正当性が検証され、コンテンツファイルCFの送信者の正当性が確認される。

【0196】ステップS46-8: 署名処理部189は、公開鍵データKCP, KSAM1, pを用いて、作業用メモリ200に記憶されている署名データSIG7, CP, SIG42, SAM1の正当性を検証する。そして、署名データSIG7, CP, SIG42, SAM1が正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

【0197】ステップS46-9: 署名処理部189は、記憶部192から読み出した公開鍵データKESC, pを用いて、図44(B)に示すキーファイルKFに格納された署名データSIGK1, ESCの正当性を確認する。そして、署名データSIGK1, ESCが正当であると検証されたときに、キーファイルKFの作成者の正当性が確認される。

【0198】ステップS46-10: 署名処理部189は、ハッシュ値HK1の正当性を検証し、キーファイルKF1の作成者および送信者の正当性を確認する。なお、当該例では、キーファイルKF1の作成者と送信元とが同じ場合を述べたが、キーファイルKF1の作成者と送信元とが異なる場合には、キーファイルKF1に対して

作成者の署名データと送信者と署名データとが作成され、署名処理部189において、双方の署名データの正当性が検証される。

【0199】ステップS46-11：利用監視部186は、ステップS46-10で復号されたキーファイルKF<sub>1</sub>に格納された利用制御データ166を用いて、以後のコンテンツデータCの購入・利用形態を制御する。

【0200】ステップS46-12：ユーザが操作部165を操作して購入形態を決定すると、それに応じた内部割り込みS810をSAM105<sub>2</sub>のCPU1100が受ける。

ステップS46-13：課金処理部187は、CPU1100からの制御に基づいて、外部メモリ201に記憶されている利用履歴データ108を更新する。また、課金処理部187は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態に応じて利用制御データ166を更新する。このとき送信元のSAMの利用制御データ166は破棄される。

【0201】ステップS46-14：暗号化・復号部173は、記憶部192から読み出した記録用鍵データKSTR、メディア鍵データK<sub>MED</sub>および購入者鍵データK<sub>PIN</sub>を順に用いて、ステップS46-12で生成された利用制御データ166を暗号化してメディア・ドライブSAM管理部855に出力する。

ステップS46-15：メディア・ドライブSAM管理部855は、新たな利用制御データ166を格納したキーファイルKF<sub>1</sub>を、セクタライズ処理、セクタヘッダの付加処理、スクランブル処理、ECCエンコード処理、変調処理および同期処理を経て、RAM型の記録媒体1304のセキュアRAM領域132に記録する。なお、メディア鍵データK<sub>MED</sub>は、図45に示す相互認証部170と図41に示すRAM型の記録媒体1304のメディアSAM133との間の相互認証によって記憶部192に事前に記憶されている。

【0202】ここで、記録用鍵データKSTRは、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc)機器などの種類(当該例では、AV機器160<sub>2</sub>)に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。なお、SACDとDVDとは、ディスク媒体の物理的な構造が同じであるため、DVD機器を用いてSACDの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データKSTRは、このような場合において、不正コピーを防止する役割を果たす。なお、本実施形態では、記録用鍵データKSTRを用いた暗号化を行わないようにしてもよい。

【0203】また、メディア鍵データK<sub>MED</sub>は、記録媒体(当該例では、RAM型の記録媒体1304)にユニークなデータである。メディア鍵データK<sub>MED</sub>は、記録

媒体(当該例では、図41に示すRAM型の記録媒体1304)側に格納されており、記録媒体のメディアSAMにおいてメディア鍵データK<sub>MED</sub>を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データK<sub>MED</sub>は、記録媒体にメディアSAMが搭載されている場合には、当該メディアSAM内に記憶されており、記録媒体にメディアSAMが搭載されていない場合には、例えば、RAM領域内の明示しないホストCPUの管理外の領域に記憶されている。なお、本実施形態のように、機器側のSAM(当該例では、SAM105<sub>2</sub>)とメディアSAM(当該例では、メディアSAM133)との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データK<sub>MED</sub>を機器側のSAMに転送し、機器側のSAMにおいてメディア鍵データK<sub>MED</sub>を用いた暗号化および復号を行なってもよい。本実施形態では、記録用鍵データKSTRおよびメディア鍵データK<sub>MED</sub>が、記録媒体の物理層のレベルのセキュリティを確保するために用いられる。

【0204】また、購入者鍵データK<sub>PIN</sub>は、コンテンツファイルCFの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してEMDサービスセクタ102によって割り当てられる。購入者鍵データK<sub>PIN</sub>は、EMDサービスセクタ102において管理される。

【0205】ステップS46-16：キーファイルKFが作業用メモリ200から読み出され、メディア・ドライブSAM管理部855を介して、図41に示すメディア・ドライブSAM260によってRAM型の記録媒体1304のセキュアRAM領域132に書き込まれる。

【0206】ステップS46-17：SAM105<sub>2</sub>のCPU1100は、上述したセキュアコンテナの入力処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。なお、CPU1100は、上述したセキュアコンテナの入力処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0207】また、上述した実施形態では、メディア・ドライブSAM260による処理を経て、キーファイルKF、KF<sub>1</sub>をRAM型の記録媒体1304のセキュアRAM領域132に記録する場合を例示したが、図41において点線で示すように、SAM105<sub>2</sub>からメディアSAM133にキーファイルKF、KF<sub>1</sub>を記録するようにしてもよい。

【0208】また、上述した実施形態では、SAM105<sub>1</sub>からSAM105<sub>2</sub>にセキュアコンテナ104xを送信する場合を例示したが、ネットワーク機器160<sub>1</sub>のホストCPUおよびAV機器160<sub>2</sub>のホストCPUによって、コンテンツファイルCFおよび権利書データ106をネットワーク機器160<sub>1</sub>からAV機器160

2に送信してもよい。この場合には、SAM105<sub>1</sub>からSAM105<sub>2</sub>に、利用制御データ166およびコンテンツ鍵データKcが送信される。

【0209】また、その他の実施形態として、例えば、SAM105<sub>1</sub>において購入形態を決定し、SAM105<sub>2</sub>では購入形態を決定せずに、SAM105<sub>1</sub>において生成した利用制御データ166をSAM105<sub>2</sub>でそのまま用いてもよい。この場合には、利用履歴データ108は、SAM105<sub>1</sub>において生成され、SAM105<sub>2</sub>では生成されない。また、コンテンツデータCの購入は、例えば、複数のコンテンツデータCからなるアルバムを購入する形態で行ってもよい。この場合に、アルバムを構成する複数のコンテンツデータCは、異なるコンテンツプロバイダ101によって提供されてもよい（後述する第2実施形態の場合には、さらに異なるサブプロバイダ310によって提供されてもよい）。また、アルバムを構成する一部のコンテンツデータCについての購入を行った後に、その他のコンテンツデータCを追加する形で購入を行い、最終的にアルバムを構成する全てのコンテンツデータCを購入してもよい。

【0210】図48は、コンテンツデータCの種々の購入形態の例を説明するための図である。図48に示すように、AV機器160<sub>3</sub>は、ネットワーク機器160<sub>1</sub>がコンテンツプロバイダ101から受信したコンテンツデータCを、権利書データ106を用いて購入し、利用制御データ166aを生成している。また、AV機器160<sub>2</sub>は、ネットワーク機器160<sub>1</sub>がコンテンツプロバイダ101から受信したコンテンツデータCを、権利書データ106を用いて購入し、利用制御データ166bを生成している。また、AV機器160<sub>3</sub>は、AV機器160<sub>2</sub>が購入したコンテンツデータCを複製し、AV機器160<sub>2</sub>で作成した利用制御データ166bを用いて利用形態を決定している。これにより、AV機器160<sub>3</sub>において、利用制御データ166cが作成される。また、AV機器160<sub>3</sub>では、利用制御データ166cから利用履歴データ108bが作成される。また、AV機器160<sub>4</sub>は、ネットワーク機器160<sub>1</sub>がコンテンツプロバイダ101から受信して購入形態を決定したコンテンツデータCを入力し、ネットワーク機器160<sub>1</sub>が作成した利用制御データ166を用いて当該コンテンツデータCの購入形態を決定する。これにより、AV機器160<sub>4</sub>において、利用制御データ166aが作成される。また、AV機器160<sub>4</sub>では、利用制御データ166aから利用履歴データ108aが作成される。なお、利用制御データ166a、166b、166cは、AV機器160<sub>4</sub>、160<sub>2</sub>、160<sub>3</sub>において、それぞれ固有の記録用鍵データSSTR、並びに記録メディア（媒体）に固有のメディア鍵データKMEDを用いて暗号化され、記録媒体に記録される。本実施形態では、ユーザは、コンテンツデータCの所有権に対して対価を

支払うのではなく、使用権に対価を支払う。コンテンツデータの複製は、コンテンツのプロモーションに相当し、マーケットの拡張という観点からコンテンツデータの権利者の要請にかなう行為となる。

【0211】＜ROM型の記録媒体のコンテンツデータの購入形態決定処理＞図49に示すように、コンテンツの購入形態が未決定の図11に示すROM型の記録媒体1301をユーザホームネットワーク303がオフラインで配給を受けた場合に、AV機器160<sub>2</sub>において購入形態を決定する際の処理の流れを図50および図51を参照しながら説明する。図51は、当該処理のフローチャートである。

ステップS51-0：ユーザによる操作部165の操作に応じて、ROM型の記録媒体を用いて配給されたコンテンツの購入形態を決定することを示す内部割り込みS810を、図50に示すSAM105<sub>2</sub>のCPU1100が受ける。

ステップS51-1：SAM105<sub>2</sub>は、図50に示す相互認証部170と図11に示すROM型の記録媒体1301のメディアSAM133との間で相互認証を行った後に、メディアSAM133からメディア鍵データKMEDを入力する。なお、SAM105<sub>2</sub>が、事前にメディア鍵データKMEDを保持している場合には、当該入力を行わなくても良い。

【0212】ステップS51-2：ROM型の記録媒体1301のセキュアRAM領域132に記録されているセキュアコンテナ104に格納された図3（B）、

（C）に示すキーファイルKFおよびその署名データSIG<sub>7</sub>CPと、公開鍵証明書データCERCPおよびその署名データSIG<sub>1</sub>ESCとを、メディア・ドライブSAM管理部855を介して入力して作業用メモリ200に書き込む。

【0213】ステップS51-3：署名処理部189において、署名データSIG<sub>1</sub>ESCの正当性を確認した後、公開鍵証明書データCERCPから公開鍵データKCPを取り出し、この公開鍵データKCPを用いて、署名データSIG<sub>7</sub>CPの正当性、すなわちキーファイルKFの送信者の正当性を検証する。また、署名処理部189において、記憶部192から読み出した公開鍵データKESCを用いて、キーファイルKFに格納された署名データSIG<sub>1</sub>GK<sub>1</sub>ESCの正当性、すなわちキーファイルKFの作成者の正当性を検証する。

【0214】ステップS51-4：署名処理部189において署名データSIG<sub>7</sub>CP、SIG<sub>1</sub>GK<sub>1</sub>ESCの正当性が確認されると、作業用メモリ200から暗号化・復号部172にキーファイルKFを読み出す。次に、暗号化・復号部172において、対応する期間のライセンス鍵データKD<sub>1</sub>～KD<sub>3</sub>を用いて、キーファイルKFに格納されたコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC

1 ~ SDC<sub>3</sub> を復号した後に、作業用メモリ 200 に書き込む。

【0215】ステップ S51-5: 図 50 に示す相互認証部 170 と図 49 に示す AV 圧縮・伸長用 SAM163 との間で相互認証を行った後に、SAM105<sub>2</sub> の AV 圧縮・伸長用 SAM 管理部 184 は、作業用メモリ 200 に記憶されているコンテンツ鍵データ Kc および権利書データ 106 に格納された半開示パラメータデータ 199、並びに ROM 型の記録媒体 130<sub>1</sub> の ROM 領域 131 から読み出したコンテンツファイル CF に格納されたコンテンツデータ C を図 49 に示す AV 圧縮・伸長用 SAM163 に出力する。次に、AV 圧縮・伸長用 SAM163 において、コンテンツデータ C がコンテンツ鍵データ Kc を用いて半開示モードで復号された後に伸長され、再生モジュール 270 に出力される。そして、再生モジュール 270 において、AV 圧縮・伸長用 SAM163 からのコンテンツデータ C が再生される。

【0216】ステップ S51-6: ユーザによる図 49 に示す操作部 165 の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す内部割り込み S810 が、SAM105<sub>2</sub> の CPU1100 に出される。

【0217】ステップ S51-7: 課金処理部 187 は、操作信号 S165 に応じた利用制御データ 166 を作成し、これを作業用メモリ 200 に書き込む。ステップ S51-8: 作業用メモリ 200 から暗号化・復号部 173 に、コンテンツ鍵データ Kc および利用制御データ 166 が出力される。暗号化・復号部 173 は、作業用メモリ 200 から入力したコンテンツ鍵データ Kc および利用制御データ 166 を、記憶部 192 から読み出した記録用鍵データ KSTR、メディア鍵データ KMED および購入者鍵データ KPIN を用いて順次に暗号化して作業用メモリ 200 に書き込む。

【0218】ステップ S51-9: メディア SAM 管理部 197 において、作業用メモリ 200 から読み出した、暗号化されたコンテンツ鍵データ Kc および利用制御データ 166 と、SAM プログラム・ダウンロード・コンテナ SDC<sub>1</sub> ~ SDC<sub>3</sub> を用いて図 44 (C) に示すキーファイル KF<sub>1</sub> が生成される。また、署名処理部 189 において、図 44 (C) に示すキーファイル KF<sub>1</sub> のハッシュ値 H<sub>K1</sub> が生成され、当該ハッシュ値 H<sub>K1</sub> がメディア・ドライブ SAM 管理部 855 に出力される。図 50 に示す相互認証部 170 と図 49 に示すメディア SAM133 との間で相互認証を行った後に、メディア・ドライブ SAM 管理部 855 は、キーファイル KF<sub>1</sub> およびハッシュ値 H<sub>K1</sub> を、図 49 に示すメディア・ドライブ SAM260 を介して ROM 型の記録媒体 130<sub>1</sub> のセキュア RAM 領域 132 に書き込む。これにより、購入形態が決定された ROM 型の記録媒体 130<sub>1</sub> が得られる。このとき、課金処理部 187 が生成した利用制御

データ 166 および利用履歴データ 108 は、所定のタイミングで、作業用メモリ 200 および外部メモリ 201 からそれぞれ読み出しされた EMD サービスセンタ 102 に送信される。なお、ROM 型の記録媒体 130<sub>1</sub> のメディア SAM133 にキーファイル KF が格納されている場合には、図 49 において点線で示されるように、SAM105<sub>2</sub> はメディア SAM133 からキーファイル KF を入力する。また、この場合に、SAM105<sub>2</sub> は、作成したキーファイル KF<sub>1</sub> をメディア SAM133 に書き込む。

【0219】ステップ S51-10: SAM105<sub>2</sub> の CPU1100 は、上述した ROM 型の記録媒体を用いて配給されたコンテンツの購入形態を決定する処理が適切に行われたか否かを、外部割込みでホスト CPU810 に通知する。なお、CPU1100 は、上述した ROM 型の記録媒体を用いて配給されたコンテンツの購入形態を決定する処理が適切に行われたか否かを示す SAM ステータスレジスタのフラグを設定し、ホスト CPU810 がポーリングによって当該フラグを読んでもよい。

【0220】<ROM 型の記録媒体のコンテンツデータの購入形態を決定した後に、RAM 型の記録媒体に書き込む場合の処理>以下、図 52 に示すように、AV 機器 160<sub>3</sub> において購入形態が未決定の ROM 型の記録媒体 130<sub>1</sub> からセキュアコンテナ 104 を読み出して新たなセキュアコンテナ 104<sub>y</sub> を生成し、これを AV 機器 160<sub>2</sub> に転送し、AV 機器 160<sub>2</sub> において購入形態を決定して RAM 型の記録媒体 130<sub>5</sub> に書き込む際の処理の流れを図 53、図 54、図 55 を参照しながら説明する。なお、ROM 型の記録媒体 130<sub>1</sub> から RAM 型の記録媒体 130<sub>5</sub> へのセキュアコンテナ 104<sub>y</sub> の転送は、図 1 に示すネットワーク機器 160<sub>1</sub> および AV 機器 160<sub>1</sub> ~ 160<sub>4</sub> のいずれの間で行ってもよい。図 55 は、当該処理のフローチャートである。

【0221】ステップ S55-0: ユーザによる操作部 165 の操作に応じて、購入形態が未決定の ROM 型の記録媒体から読み出したセキュアコンテナを SAM105<sub>2</sub> に転送することを示す内部割り込み S810 を、図 53 に示す CPU1100 が受ける。

ステップ S55-1: SAM105<sub>3</sub> は、SAM 登録リストを検証し、セキュアコンテナの転送先の SAM105<sub>2</sub> が正規に登録されている SAM であるか否かを検証し、正規に登録されていると判断した場合にステップ S55-2 以降の処理を行う。また、SAM105<sub>3</sub> は、SAM105<sub>2</sub> がホームネットワーク内の SAM であるか否かの検証を行う。

ステップ S55-2: SAM105<sub>3</sub> と SAM105<sub>2</sub> との間で相互認証が行われ、セッション鍵データ KSES が共有される。

【0222】ステップ S55-3: AV 機器 160<sub>3</sub> の SAM105<sub>3</sub> と ROM 型の記録媒体 130<sub>1</sub> のメディア

アSAM133との間で相互認証を行い、ROM型の記録媒体130<sub>1</sub>のメディア鍵データK<sub>MED1</sub>をSAM105<sub>3</sub>に転送する。なお、メディア鍵データK<sub>MED1</sub>を用いた暗号化をROM型の記録媒体130<sub>1</sub>のメディアSAM133において行う場合には、メディア鍵データK<sub>MED1</sub>の転送は行われない。

【0223】ステップS55-4: AV機器160<sub>2</sub>のSAM105<sub>2</sub>とRAM型の記録媒体130<sub>5</sub>のメディアSAM133との間で相互認証を行い、RAM型の記録媒体130<sub>5</sub>のメディア鍵データK<sub>MED2</sub>をSAM105<sub>2</sub>に転送する。なお、メディア鍵データK<sub>MED2</sub>を用いた暗号化をRAM型の記録媒体130<sub>5</sub>のメディアSAM133において行う場合には、メディア鍵データK<sub>MED2</sub>の転送は行われない。

【0224】ステップS55-5: SAM105<sub>3</sub>は、図53に示すように、メディア・ドライブSAM管理部855を介して、ROM型の記録媒体130<sub>1</sub>のROM領域131からコンテンツファイルCFおよびその署名データSIG<sub>6</sub>, CPを読み出し、これをSAM管理部190に出力すると共に、署名処理部189において、秘密鍵データK<sub>SAM3</sub>, Sを用いて、これらの署名データSIG<sub>350</sub>, SAM3を作成する。

【0225】ステップS55-6: SAM105<sub>3</sub>は、図53に示すように、メディア・ドライブSAM管理部855を介して、ROM型の記録媒体130<sub>1</sub>のセキュアRAM領域132からキーファイルKFおよびその署名データSIG<sub>7</sub>, CPを読み出し、これをSAM管理部190に出力すると共に、署名処理部189において、秘密鍵データK<sub>SAM3</sub>, Sを用いて、これらの署名データSIG<sub>352</sub>, SAM3が作成される。

【0226】ステップS55-7: SAM105<sub>3</sub>において、記憶部192からSAM管理部190に公開鍵証明書データCER<sub>SAM3</sub>およびその署名データSIG<sub>351</sub>, ESCを読み出される。

【0227】ステップS55-8: SAM105<sub>3</sub>の例えばSAM管理部190において、図54に示すセキュアコンテナ104yが作成される。

【0228】ステップS55-9: SAM105<sub>3</sub>の暗号化・復号部171において、ステップS55-2で得たセッション鍵データK<sub>SES</sub>を用いて、セキュアコンテナ104yが暗号化される。

【0229】ステップS55-10: SAM105<sub>3</sub>のSAM管理部190からAV機器160<sub>2</sub>に、セキュアコンテナ104yが出力される。そして、SAM105<sub>3</sub>のCPU1100からホストCPU810に、外部割り込みで、上述した処理が適切に行われたか否かが通知される。なお、CPU1100は、上述した処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。SAM105<sub>2</sub>では、ホ

ストCPU810からの内部割り込みS810によるCPU1100の制御によって、図57に示すように、SAM管理部190を介してSAM105<sub>3</sub>から入力した図54に示すセキュアコンテナ104yが暗号化・復号部171においてセッション鍵データK<sub>SES</sub>を用いて復号される。そして、当該復号されたセキュアコンテナ104y内のキーファイルKFおよびその署名データSIG<sub>7</sub>, CP, SIG<sub>350</sub>, SAM3と、公開鍵証明書データCER<sub>SAM3</sub>およびその署名データSIG<sub>351</sub>, ESCと、公開鍵証明書データCER<sub>CP</sub>およびその署名データSIG<sub>1</sub>, ESCとが、作業用メモリ200に書き込まれる。

【0230】ステップS55-12: SAM105<sub>2</sub>の署名処理部189において、セキュアコンテナ104y内に格納された署名データSIG<sub>6</sub>, CP, SIG<sub>350</sub>, SAM3の正当性、すなわちコンテンツファイルCFの作成者および送信者の正当性を確認する。

ステップS55-13: コンテンツファイルCFの作成者および送信者が正当であると確認された後に、メディア・ドライブSAM管理部855を介してRAM型の記録媒体130<sub>5</sub>のRAM領域134にコンテンツファイルCFが書き込まれる。なお、コンテンツファイルCFは、ホストCPU810の制御によって、SAMを介さずに、RAM型の記録媒体130<sub>5</sub>のRAM領域134に直接的に記録してもよい。

【0231】ステップS55-14: 署名処理部189において、署名データSIG<sub>351</sub>, ESCが署名検証され、公開鍵証明書データCER<sub>SAM3</sub>の正当性が確認された後に、公開鍵証明書データCER<sub>SAM3</sub>に格納された公開鍵データK<sub>SAM3</sub>および公開鍵データK<sub>ESC</sub>, Pを用いて、署名データSIG<sub>7</sub>, CP, SIG<sub>352</sub>, SAM3, SIG<sub>K1</sub>, ESCの正当性、すなわちキーファイルKFの作成者および送信者の正当性が確認される。

【0232】ステップS55-15: キーファイルKFの作成者および送信者の正当性が確認されると、作業用メモリ200からキーファイルKFが読み出されて暗号化・復号部172に出力され、暗号化・復号部172において、ライセンス鍵データKD<sub>1</sub>〜KD<sub>3</sub>を用いて復号された後に、作業用メモリ200に書き込まれる。

【0233】ステップS55-16: 作業用メモリ200に記憶されている既に復号されたキーファイルKFに格納された権利書データ106が、利用監視部186に出力される。そして、利用監視部186において、権利書データ106に基づいて、コンテンツの購入形態および利用形態が管理（監視）される。

【0234】ステップS55-17: ユーザによって図52に示す操作部165の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた内部割り込みS810が、ホストCPU810からSAM105<sub>2</sub>のCPU1100に出される。ステップS55-18: 課金処理部187において、決

定された購入・利用形態に応じて利用制御データ166および利用履歴データ108が生成され、これが作業用メモリ200および外部メモリ201にそれぞれ書き込まれる。利用制御データ166および利用履歴データ108は、所定のタイミングで、EMDサービスセンタ102に送信される。

【0235】ステップS55-19:コンテンツ鍵データKcおよび利用制御データ166が、作業用メモリ200から暗号化・復号部173に読み出され、暗号化・復号部173において記憶部192から読み出した記録用鍵データKSTR、メディア鍵データKMED2および購入者鍵データKPINを用いて順に暗号化され、メディアSAM管理部197に出力される。また、作業用メモリ200からメディアSAM管理部197に、キーファイルKFが出力される。

【0236】ステップS55-20:メディアSAM管理部197において、図44(C)に示すキーファイルKF<sub>1</sub>が作成され、キーファイルKF<sub>1</sub>がメディアSAM管理部197を介してRAM型の記録媒体1305のメディアSAM133に書き込まれる。また、メディアSAM管理部197を介して、キーファイルKFがRAM型の記録媒体1305のメディアSAM133に書き込まれる。

【0237】ステップS55-21: SAM105<sub>2</sub>のCPU1100は、上述した処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。なお、CPU1100は、上述した処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0238】以下、SAM105<sub>1</sub>~105<sub>4</sub>の実現方法について説明する。SAM105<sub>1</sub>~105<sub>4</sub>の機能を実ハードウェアとして実現する場合は、メモリを内蔵したASIC型のCPUを用いて、そのメモリには、図2に示す各機能を実現するためのセキュリティ機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密性の高いデータが格納される。暗号ライブラリモジュール(公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数)、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【0239】例えば、図2に示す暗号化・復号部171などのモジュールは、例えば、処理速度の問題でハードウェアとしてASIC型のCPU内のIPコアとして実装される。クロック速度やCPUコード体系などの性能によっては、暗号化・復号部171をソフトウェアとして実装してもよい。また、図2に示す記憶部192や、図2に示す機能を実現するためのプログラムモジ

ュールおよびデータを格納するメモリとしては、例えば、不揮発メモリ(フラッシュROM)が用いられ、作業用メモリとしてはSRAMなどの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM105<sub>1</sub>~105<sub>4</sub>に内蔵されるメモリとして、強誘電体メモリ(FeRAM)を用いてもよい。また、SAM105<sub>1</sub>~105<sub>4</sub>には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【0240】上述したように、SAM105<sub>1</sub>~105<sub>4</sub>は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM105<sub>1</sub>~105<sub>4</sub>を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側のメモリー空間を管理するMMU(Memory Management Unit)を用いて、搭載機器側のホストCPUからは見えないアドレス空間を設定する。また、SAM105<sub>1</sub>~105<sub>4</sub>は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール(ハードウェアICE、ソフトウェアICE)などを用いたリアルタイムデバッグ(リバースエンジニアリング)が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。SAM105<sub>1</sub>~105<sub>4</sub>自身は、ハードウェア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

【0241】SAM105<sub>1</sub>~105<sub>4</sub>の機能を全てソフトウェアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウェア処理を行う場合と、通常のセットに搭載されているホストCPU上のソフトウェア処理で行い、当該処理のときのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様と考えられる。一方、後者は、タンパレスタントソフトウェアと呼ばれるもので、ICE(デバッグ)で実行状況を解読されても、そのタスクの実行順序がバラバラであったり(この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のライン



に影響がでないようにタスク切りを行う)、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ(MiniOS)と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【0242】次に、図2に示すAV圧縮・伸長用SAM163は、図2に示すように、AV圧縮・伸長用SAM163は、相互認証部220、復号部221、復号部222、伸長部223、電子透かし情報処理部224および半開示処理部225を有する。相互認証部220は、AV圧縮・伸長用SAM163がSAM105<sub>1</sub>からデータを入力する際に、図30に示す相互認証部170との間で相互認証を行ってセッション鍵データK<sub>SES</sub>を生成する。

【0243】復号部221は、SAM105<sub>1</sub>から入力したコンテンツ鍵データK<sub>C</sub>、半開示パラメータデータ199、ユーザ電子透かし情報用データ196およびコンテンツデータCを、セッション鍵データK<sub>SES</sub>を用いて復号する。そして、復号部221は、復号したコンテンツ鍵データK<sub>C</sub>およびコンテンツデータCを復号部222に出力し、復号したユーザ電子透かし情報用データ196を電子透かし情報処理部224に出力し、半開示パラメータデータ199を半開示処理部225に出力する。

【0244】復号部222は、半開示処理部225からの制御に基づいて、コンテンツ鍵データK<sub>C</sub>を用いて、コンテンツデータCを半開示状態で復号し、復号したコンテンツデータCを伸長部223に出力する。また、復号部222は、通常動作時にコンテンツデータCの全体をコンテンツ鍵データK<sub>C</sub>で復号する。

【0245】伸長部223は、復号されたコンテンツデータCを伸長して、電子透かし情報処理部224に出力する。伸長部223は、例えば、図3(A)に示すコンテンツファイルCFに格納されたA/V伸長用ソフトウェアを用いて伸長処理を行い、例えば、ATRAC3方式で伸長処理を行う。

【0246】電子透かし情報処理部224は、復号されたユーザ電子透かし情報用データ196に応じたユーザ電子透かし情報を、復号されたコンテンツデータCに埋め込み、新たなコンテンツデータCを生成する。電子透かし情報処理部224は、当該新たなコンテンツデータCを再生モジュール169に出力する。このように、ユーザ電子透かし情報は、コンテンツデータCを再生するときに、AV圧縮・伸長用SAM163において埋め込まれる。なお、本発明では、コンテンツデータCにユーザ電子透かし情報用データ196を埋め込まないようにしてもよい。

【0247】半開示処理部225は、半開示パラメータデータ199に基づいて、例えば、コンテンツデータCのうち復号を行わないブロックと、復号を行うブロック

とを復号部222に指示する。また、半開示処理部225は、その他に、半開示パラメータデータ199に基づいて、試験時の再生機能を限定したり、試験可能な期間を限定するなどの制御を行う。

【0248】再生モジュール169は、復号および伸長されたコンテンツデータCに応じた再生を行う。

【0249】以下、SAM105<sub>1</sub>~105<sub>4</sub>の出荷時におけるEMDサービスセンタ102への登録処理について説明する。なお、SAM105<sub>1</sub>~105<sub>4</sub>の登録処理は同じであるため、以下、SAM105<sub>1</sub>の登録処理について述べる。SAM105<sub>1</sub>の出荷時には、EMDサービスセンタ102の鍵サーバ141によって、SAM管理部149を介して、図30などに示す記憶部192に以下に示す鍵データが初期登録される。また、SAM105<sub>1</sub>には、例えば、出荷時に、記憶部192などに、SAM105<sub>1</sub>がEMDサービスセンタ102に初回にアクセスする際に用いられるプログラムなどが記憶される。すなわち、記憶部192には、例えば、図34において左側に「\*」が付されているSAM105<sub>1</sub>の識別子SAM\_ID、記録用鍵データK<sub>STR</sub>、ルート認証局2の公開鍵データK<sub>R-CA</sub>、EMDサービスセンタ102の公開鍵データK<sub>ESC,P</sub>、SAM105<sub>1</sub>の秘密鍵データK<sub>SAM1,S</sub>、公開鍵証明書データC<sub>ER</sub>SAM1およびその署名データS1G22、ESC、AV圧縮・伸長用SAM163およびメディアSAMとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。なお、公開鍵証明書データC<sub>ER</sub>SAM1は、SAM105<sub>1</sub>を出荷後に登録する際にEMDサービスセンタ102からSAM105<sub>1</sub>に送信してもよい。

【0250】また、記憶部192には、SAM105<sub>1</sub>の出荷時に、図3に示すコンテンツファイルCFおよびキーファイルKFを読み込み形式を示すファイルリダが、EMDサービスセンタ102によって書き込まれる。SAM105<sub>1</sub>では、コンテンツファイルCFおよびキーファイルKFに格納されたデータを利用する際に、記憶部192に記憶されたファイルリダが用いられる。

【0251】ここで、ルート認証局2の公開鍵データK<sub>R-CA</sub>は、インターネットの電子商取引などでは一般的に使用されているRSAを使用し、データ長は例えば1024ビットである。公開鍵データK<sub>R-CA</sub>は、図1に示すルート認証局2によって発行される。また、EMDサービスセンタ102の公開鍵データK<sub>ESC,P</sub>は、短いデータ長でRSAと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば160ビットである。但し、暗号化の強度を考慮すると、公開鍵データK<sub>ESC,P</sub>は192ビット以上であることが望ましい。また、EMDサービスセンタ102は、ルート認証局2に公開鍵データK<sub>ESC,P</sub>を登録する。また、ルート認証局2は、公開鍵データK<sub>ESC,P</sub>の公開鍵証明

書データCERESCを作成する。公開鍵データKESC,Pを格納した公開鍵証明書データCERESCは、好ましく、SAM1051の出荷時に記憶部192に記憶される。この場合に、公開鍵証明書データCERESCは、ルート認証局92の秘密鍵データKROOT,Sで署名されている。

【0252】 EMDサービスセンタ102は、乱数を発生してSAM1051の秘密鍵データKSA1,S、を生成し、これとペアとなる公開鍵データKSA1,Pを生成する。また、EMDサービスセンタ102は、ルート認証局92の認証をもらって、公開鍵データKSA1,Pの公開鍵証明書データCERSA1を発行し、これに自らの秘密鍵データKESC,Sを用いて署名データを添付する。すなわち、EMDサービスセンタ102は、セカンダCA(認証局)として機能を果たす。

【0253】 また、SAM1051には、EMDサービスセンタ102により、EMDサービスセンタ102の管理下にある一意(ユニーク)な識別子SAM\_IDが割り当てられ、これがSAM1051の記憶部192に格納されると共に、EMDサービスセンタ102によって管理される。

【0254】 また、SAM1051は、出荷後、例えば、ユーザによってEMDサービスセンタ102と接続され、登録手続を行うと共に、EMDサービスセンタ102から記憶部192にライセンス鍵データKD1~KD3が転送される。すなわち、SAM1051を利用するユーザは、コンテンツをダウンロードする前にEMDサービスセンタ102に登録手続が必要である。この登録手続は、例えば、SAM1051を搭載している機器(当該例では、ネットワーク機器1601)を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報(ユーザの氏名、住所、連絡先、性別、決済口座、ログイン名、パスワードなど)を記載して例えば郵便などのおフラインで行なわれる。SAM1051は、上述した登録手続を経た後でないと使用できない。

【0255】 EMDサービスセンタ102は、SAM1051のユーザによる登録手続に応じて、ユーザに固有の識別子USER\_IDを発行し、例えば、SAM\_IDとUSER\_IDとの対応関係を管理し、該金時に利用する。また、EMDサービスセンタ102は、SAM1051のユーザに対して情報参照識別子IDと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照識別子IDとパスワードを用いて、EMDサービスセンタ102に、例えば現在までのコンテンツデータの利用状況(利用履歴)などを情報の問い合わせを行なうことができる。また、EMDサービスセンタ102は、ユーザの登録時に、クレジットカード会社などに身分の確認を行ったり、オフラインで本人の確認を行なう。

【0256】 次に、図34に示すように、SAM1051内の記憶部192にSAM登録リストを格納する手順について説明する。図1に示すSAM1051は、例えば、バス191としてIEEE1394シリアルバスを用いた場合に、バス191に接続された機器の電源を立ち上げたり、新しい機器をバス191に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するSAM1052~SAM1054のSAM登録リストを得る。なお、IEEE1394シリアルバスであるバス191に応じて生成されたトポロジーマップは、例えば、図58に示すように、バス191にSAM1051~1054に加えてAV機器1605、1606のSCMS処理回路1055、1056が接続されている場合に、SAM1051~1054およびSCMS処理回路1055、1056を対象として生成される。従って、SAM1051は、当該トポロジーマップから、SAM1051~1054についての情報を抽出して図59に示すSAM登録リストを生成する。

【0257】 そして、SAM1051は、図59に示すSAM登録リストを、EMDサービスセンタ102に登録して署名を得る。これらの処理は、バス191のセッションを利用してSAM1051が自動的にを行い、EMDサービスセンタ102にSAM登録リストの登録命令を発行する。EMDサービスセンタ102は、SAM1051から図59に示すSAM登録リストを受けると、有効期限を確認する。そして、EMDサービスセンタ102は、登録時にSAM1051より指定された決済機能の有無を参照して対応する部分の設定を行う。また、EMDサービスセンタ102は、予め保持している図60に示すリボケーションリストCRLをチェックしてSAM登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にEMDサービスセンタ102によって使用が禁止されている(無効な)SAMのリストである。各SAMは他のSAMと通信を行う際に、リボケーションリストによって通信相手のSAMが無効にされている場合には、当該通信相手のSAMとの通信を停止する。また、EMDサービスセンタ102は、決済時にはSAM1051に対応するSAM登録リストを取り出し、その中に記述されたSAMがリボケーションリストに含まれているかを確認する。また、EMDサービスセンタ102は、SAM登録リストに署名を添付する。これにより、図61に示すSAM登録リストが作成される。なお、SAMリボケーションリストは、同一系の(同一のバス191に接続されている)SAMのみを対象として生成され、各SAMに対応するリボケーションフラグによって、当該SAMの有効および無効を示している。

【0258】 なお、リボケーションリストCRLの更新は、例えば、EMDサービスセンタ102からSAMに放送される更新データに応じて、SAM内部で自動的に

行なうことが好ましい。

【0259】以下、SAMが持つセキュリティ機能について説明する。SAMは、セキュリティに関する機能として、共通鍵暗号方式のDES (Triple DES/AES)、公開鍵暗号方式の楕円曲線暗号 (署名生成/検証 ECD SA、共有鍵生成 ECD-H、公開鍵暗号 EC-EI gamal)、圧縮関数のハッシュ関数 SHA-1、乱数生成器 (真性乱数) の暗号ライブラリーのIP部品を有している。相互認証、署名生成、署名検証、共有鍵 (セッション鍵) 作成 (配送) には公開鍵暗号方式 (楕円曲線暗号) が用いられ、コンテンツの暗号、復号には共通鍵暗号 (DES) が用いられ、署名生成、検証の中のメッセージ認証に圧縮関数 (ハッシュ関数) が用いられる。

【0260】図62は、SAMが持つセキュリティ機能の説明するための図である。SAMが管理するセキュリティ機能は、コンテンツに関連する暗号、復号処理をつかさどるアプリケーション層でのセキュリティ機能

(1) と、通信相手と相互認証をしてセキュアな通信路を確保する物理層のセキュリティ機能 (2) との2種類がある。EMDシステム100では、配信されるコンテンツデータCはすべて暗号化され、決済と同時に鍵の購入手続きをすることを前提としている。権利客データ106は、コンテンツデータCと一緒にイン・バンド方式で送られることを前提としているので、ネットワークの媒体と関係のない層でそのデータが管理され、衛星、地上波、ケーブル、無線、記録媒体 (メディア) などの流通経路によらず、共通な権利処理システムを提供できる。具体的には、権利客データ106をネットワークの物理層のプロトコルのヘッダに挿入し入ると、使用するネットワークによって、挿入するデータが同じでも、ヘッダのどこに挿入するかを各々のネットワークで決めるといえない。

【0261】本実施形態では、コンテンツデータCおよびキーファイルKFの暗号化は、アプリケーション層での保護を意味している。相互認証は、物理層やトランスポート層で行ってもよいし、アプリケーション層で行ってもよい。物理層に暗号機能を組み込むことは、使用するハードウェアに暗号機能を組み込むことを意味している。送信、受信の両者間のセキュアな通信路を確保することが相互認証の本来の目的なので物理層で実現できることが望ましいが、実際はトランスポート層で実現し、伝送路によらないレベルでの相互認証が多い。

【0262】SAMが実現するセキュリティ機能には、通信先の相手の正当性を確認するための相互認証と、アプリケーション層での課金処理をとまなコンテンツデータの暗号化および復号とがある。機器間で通信を行う際のSAM相互間での相互認証は、通常、アプリケーション層レベルに実装されるが、トランスポート層や物理層などの他のレイヤに実装されてもよい。物理層に実装する相互認証は、5C1394CP (Content Protecti

on) を利用する。1394CPは1394LINKIC (ハードウェア) のIsochronous Channel に共通鍵暗号であるM6が実装されており、Asynchronous Channel による相互認証 (楕円曲線暗号、ハッシュ関数を利用した共通鍵暗号) の結果、生成されるセッション鍵をIsochronous Channel のM6に転送し、M6による共通鍵暗号を実現する。

【0263】SAM相互間の相互認証を物理層のハードウェア上に実装する場合には、公開鍵暗号 (楕円曲線暗号) を利用した相互認証で生成されたセッション鍵をホストCPUを介して5C1394LINKICのM6に転送し、1394CPで生成されたセッション鍵と併用してコンテンツデータの暗号化を行う。また、SAM相互間の相互認証をアプリケーション層で行う場合には、SAM内部の共通鍵暗号ライブラリ (DES/Triple DES/AES) を使って暗号化を行う。

【0264】本実施形態では、例えば、SAM相互間の相互認証をアプリケーション層に実装し、1394CPによる相互認証を1394LINKICという物理層 (ハードウェア) に実装する。この場合に、課金処理をとまなコンテンツデータの暗号化および復号はアプリケーション層で行われるが、アプリケーション層は一般ユーザから簡単にアクセスでき、時間無制限に解析される可能性があるため、当該課金処理をとまな処理に関しては、本実施形態では、外部から処理内容をいっさいモニタ (監視) できない耐タンパ性をもったハードウェア内部で行っている。これがSAMを耐タンパ性の構造を持ったハードウェアで実現する最大の理由である。なお、当該課金処理をホストCPU内で行う場合は、CPUに耐タンパ性のソフトウェアを実装する。

【0265】以下、図1に示すユーザホームネットワーク103内の例えばネットワーク機器160<sub>1</sub> 内の各種のSAMに搭載形態の一例を図63を参照しながら説明する。図63に示すように、ネットワーク機器160<sub>1</sub> 内には、ホストCPU810<sub>1</sub>、SAM105<sub>1</sub>、ダウンロードメモリ167、メディア・ドライブSAM260、ドライブCPU1003、DRAMなどのショックブルーフ (Shock Proof: 耐振動用) メモリ1004を有する。ダウンロードメモリ167と、ショックブルーフメモリ1004の一部の記憶領域は、SAM105<sub>1</sub> およびホストCPU810<sub>1</sub> の双方からアクセス可能な共有メモリとして用いられる。ショックブルーフメモリ1004は、データバス1002を介して入力したコンテンツデータを蓄積した後にAV圧縮・伸長用SAM163に出力することで、記録媒体130からのコンテンツデータの読み出し動作が振動などに要因で途切れた場合でも、AV圧縮・伸長用SAM163に連続してコンテンツデータCを出力することを可能にする。これによって、コンテンツデータの再生出力が途切れることが効果的に回避される。

【0266】ダウンロードメモリ167は、メモリコントローラ、バスアービタおよびブリッジの機能を持つモジュール1005を介して、ホストCPUバス1000に接続されている。図64は、モジュール1005の内部およびその周辺の構成を詳細に示した図である。図64に示すように、モジュール1005は、コントローラ1500およびバスアービタ/バスブリッジ1501を有する。コントローラ1500は、ダウンロードメモリ167としてDRAMを用いた場合に、DRAM1/Fとして機能し、ダウンロードメモリ167との間にr/w線、アドレスバス、CAS線およびRAS線を有している。バスアービタ/バスブリッジ1501は、ホストCPUバス1000のアービトレーション等を行い、ダウンロードメモリ167との間にデータバスを有し、コントローラ1500との間にr/w線、アドレスバスおよびReady線を有し、SAM1051との間にCS(Chip Select)線、r/w線、アドレスバス、データバスおよびReady線を有し、ホストCPUバス1000に接続されている。ホストCPUバス1000には、バスアービタ/バスブリッジ1501、ホストCPU8101およびSAM1051が接続されている。ホストCPUバス1000は、CS線、r/w線、アドレスバス、データバスおよびReady線を有する。

【0267】ダウンロードメモリ167およびショックブルーフメモリ1004には、前述したコンテンツファイルCFおよびキーマイルKFなどが記憶される。ショックブルーフメモリ1004の記憶領域のうち共有メモリとしては用いられる記憶領域以外の記憶領域は、データバス1002を介してメディア・ドラブSAM260から入力したコンテンツデータをAV圧縮・伸長用SAM163に出力するまで一時的に記憶するために用いられる。

【0268】AV圧縮・伸長用SAM163は、ホストCPUバス1000を介してダウンロードメモリ167との間でデータ転送を行い、データバス1002を介してメディア・ドラブSAM260との間でデータ転送を行う。

【0269】ホストCPUバス1000には、ダウンロードメモリ167の他に、SAM1051、AV圧縮・伸長用SAM163およびDMA(Direct Memory Access)1010が接続されている。DMA1010は、ホストCPUバス1000を介してダウンロードメモリ167へのアクセスを、ホストCPU8101からの命令に応じて、統制的に制御する。また、ホストCPUバス1000は、1394シリアル・インターフェースのL1NK層を用いてユーザホームネットワーク103内の他のSAM1052~1054と通信を行なう際に用いられる。

【0270】ドライブCPUバス1001には、ドライブCPU1003、メディア・ドラブSAM260、R

Fアンブ1006、メディアSAMインターフェイス1007およびDMA1011が接続されている。ドライブCPU1003は、例えば、ホストCPU8101からの命令を受けて、ディスク型の記録媒体130にアクセスを行う際の処理を統制的に制御する。この場合に、ホストCPU8101がマスタとなり、ドライブCPU1003がスレーブとなる。ドライブCPU1003は、ホストCPU8101から見てI/Oとして扱われる。ドライブCPU1003は、例えばRAM型などの記録媒体130にアクセスを行う際のデータのエンコードおよびデコードを行う。ドライブCPU1003は、RAM型の記録媒体130がドライブにセットされると、RAM型の記録媒体130がSAM1051による権利処理の対象となる(EMDシステム100の対象となる)記録媒体であるか否かを判断し、当該記録媒体であると判断した場合に、そのことをホストCPU8101に通知すると共に、メディア・ドラブSAM260にメディアSAM133との間の相互認証などを行うことを指示する。

【0271】メディアSAMインターフェイス1007は、ドライブCPUバス1001を介した記録媒体130のメディアSAM133に対してのアクセスを行う際のインターフェイスとして機能する。DMA1011は、例えば、ドライブCPU1003からの命令に応じて、ドライブCPUバス1001およびデータバス1002を介したショックブルーフメモリ1004へのメモリアccessを統制的に制御する。DMA1011は、例えば、データバス1002を介した、メディア・ドラブSAM260とショックブルーフメモリ1004との間のデータ転送を制御する。

【0272】図63に示す構成では、例えば、SAM1051と記録媒体130のメディアSAM133との間で相互認証などの通信の場合には、ホストCPU8101の制御に基づいて、ホストCPUバス1000、ホストCPU8101、ドライブCPU1003内のレジスタ、ドライブCPUバス1001およびメディアSAMインターフェイス1007を介して、SAM1051とメディアSAM133との間でデータが転送される。また、記録媒体130にアクセスを行う場合には、メディア・ドラブSAM260とメディアSAM133との間で相互認証が行われる。また、前述したように、ダウンロードメモリ167およびショックブルーフメモリ1004にアクセスを行うために、AV圧縮・伸長用SAM163においてデータを圧縮または伸長する場合には、SAM1051とAV圧縮・伸長用SAM163との間で相互認証が行われる。

【0273】本実施形態では、図63において、SAM1051およびAV圧縮・伸長用SAM163は、ホストCPU8101からは、I/Oインターフェイスに接続されたデバイスとして扱われる。SAM1051およ

びAV圧縮・伸長用SAM163とホストCPU810<sub>1</sub>との間の通信およびデータ転送は、メモリI/O&アドレスデコーダ1020の制御に基づいて行われる。このとき、ホストCPU810<sub>1</sub>がマスタ(Master)になり、SAM105<sub>1</sub>およびAV圧縮・伸長用SAM163がスレーブ(Slave)になる。SAM105<sub>1</sub>およびAV圧縮・伸長用SAM163は、ホストCPU810<sub>1</sub>からの命令に基づいて要求された処理を行い、必要に応じて、当該処理の結果をホストCPU810<sub>1</sub>に通知する。また、メディアSAM133およびメディア・ドラブSAM260は、ドライブCPU1003からはI/Oインターフェイスに接続されたデバイスとして扱われる。メディアSAM133およびメディア・ドラブSAM260とドライブCPU1003との間の通信およびデータ転送は、メモリI/O&アドレスデコーダ1021の制御に基づいて行われる。このとき、ドライブCPU1003がマスタになり、メディアSAM133およびメディア・ドラブSAM260がスレーブになる。メディアSAM133およびメディア・ドラブSAM260は、ドライブCPU1003からの命令に基づいて要求された処理を行い、必要に応じて、当該処理の結果をドライブCPU1003に通知する。

【0274】また、ダウンロードメモリ167およびショックブルーフメモリ1004に対してのコンテンツファイルCFおよびキーフイルKFに関するアクセス制御は、SAM105<sub>1</sub>が統括的に実行してもよいし、あるいはコンテンツファイルCFのアクセス制御をホストCPU810<sub>1</sub>が行い、キーフイルKFのアクセス制御をSAM105<sub>1</sub>が行ってもよい。

【0275】ドライブCPU1003によって記録媒体130から読み出されたコンテンツデータCは、RFアンプ1006およびメディア・ドラブSAM260を経て、ショックブルーフメモリ1004に格納され、その後、AV圧縮・伸長用SAM163において伸長される。伸長されたコンテンツデータはD/A変換器において、2でデジタルからアナログに変換され、当該変換によって得られたアナログ信号に応じた音響がスピーカから出力される。このとき、ショックブルーフメモリ1004は、記録媒体130の降散的に位置する記録領域から非連続的に読み出された複数のトラックのコンテンツデータCを一時的に格納した後に、AV圧縮・伸長用SAM163に連続して出力してもよい。

【0276】以下、図63に示すユーザホームネットワーク103内の各種のSAMのマスタ・スレーブ関係を説明する。例えば、購入形態を決定したコンテンツデータを記録媒体130に記録する場合には、図65に示すように、ホストCPU810<sub>1</sub>が、そのI/OデバイスであるSAM105<sub>1</sub>に、当該コンテンツデータの購入形態決定を行う旨を内部割り込みによって指示すると共に、記録媒体130のメディアSAM133と相互認証

を行って、記録媒体130にコンテンツデータを記録する。このとき、ホストCPU810<sub>1</sub>がマスタとなり、SAM105<sub>1</sub>および記録媒体130がスレーブとなる。記録媒体130も、ホストCPU810<sub>1</sub>からはI/Oデバイスとして扱われる。SAM105<sub>1</sub>は、ホストCPU810<sub>1</sub>から上記内部割り込みを受けると、記録媒体130のメディアSAM133と通信を行って、コンテンツデータの購入形態を決定すると共に、コンテンツ鍵データKcなどの所定の鍵データをメディアSAM133に書き込む。そして、SAM105<sub>1</sub>は、当該処理が終了すると、ホストCPU810<sub>1</sub>に対しての外部割り込み、あるいはホストCPU810<sub>1</sub>からのポーリングによって、当該処理の結果をホストCPU810<sub>1</sub>に通知する。

【0277】また、例えば、記録媒体に記録された既に購入形態が決定されたコンテンツデータの再生を行う場合には、図66に示すように、ホストCPU810<sub>1</sub>からSAM105<sub>1</sub>に対して、当該再生を行う旨の指示が内部割り込みによって出される。SAM105<sub>1</sub>は、当該内部割り込みを受けると、記録媒体130のメディアSAM133からキーフイルKFなどの鍵データブロックを読み出し、当該鍵データブロックに格納された利用制御データ166などに基づいて、コンテンツデータの再生処理を行う。SAM105<sub>1</sub>は、AV圧縮・伸長用SAM163に、記録媒体130から読み出したコンテンツデータの伸長処理を行う旨の指示を内部割り込みによって出す。AV圧縮・伸長用SAM163は、当該内部割り込みを受けると、SAM105<sub>1</sub>から受けると、記録媒体130から読み出したコンテンツデータのデスクランブル処理、電子透かし情報の埋め込み処理および検出処理、並びに伸長処理を行った後に、当該コンテンツデータをD/A変換回路などを介して出力して再生を行う。そして、AV圧縮・伸長用SAM163は、当該再生処理が終了すると、その旨をSAM105<sub>1</sub>に通知する。SAM105<sub>1</sub>は、AV圧縮・伸長用SAM163から、当該再生処理が終了した旨の通知を受けると、その旨を外部割り込み等でホストCPU810<sub>1</sub>に通知する。この場合には、ホストCPU810<sub>1</sub>とSAM105<sub>1</sub>との関係では、ホストCPU810<sub>1</sub>がマスタとなり、SAM105<sub>1</sub>がスレーブとなる。また、SAM105<sub>1</sub>とAV圧縮・伸長用SAM163との関係では、SAM105<sub>1</sub>がマスタとなり、AV圧縮・伸長用SAM163がスレーブとなる。また、上述した実施形態では、AV圧縮・伸長用SAM163をSAM105<sub>1</sub>のスレーブとなるようにしたが、AV圧縮・伸長用SAM163をホストCPU810<sub>1</sub>のスレーブとなるようにしてもよい。

【0278】また、例えば、コンテンツデータの権利処理を行うことなく、記録媒体130に記録されたコンテンツデータの再生処理を行う場合には、図67に示すよ

うに、ホストCPU810<sub>1</sub>からAV圧縮・伸長用SAM163に、内部割り込みによって、再生処理を行う旨の指示が出される。また、ホストCPU810<sub>1</sub>からメディア・ドラブSAM260に、内部割り込みによって、記録媒体130からコンテンツデータを読み出す旨の指示が出される。メディア・ドラブSAM260は、上記内部割り込みを受けると、記録媒体130から読み出したコンテンツデータをデコードしてデコードした後、ショックブルーフメモリ1004に格納する。そして、メディア・ドラブSAM260は、当該処理を終了すると、その旨を外部割り込みによってホストCPU810<sub>1</sub>に通知する。ショックブルーフメモリ1004に格納されたコンテンツデータは、AV圧縮・伸長用SAM163によって読み出され、AV圧縮・伸長用SAM163において、デスクランブル処理、電子透かし情報の埋め込み処理および検出処理、並びに伸長処理を行った後に、D/A変換回路などを介して再生出力される。AV圧縮・伸長用SAM163は、当該再生処理が終了すると、その旨を外部割り込みによってホストCPU810<sub>1</sub>に通知する。この場合に、ホストCPU810<sub>1</sub>がマスタとなり、AV圧縮・伸長用SAM163およびメディア・ドラブSAM260がスレーブとなる。

【0279】以下、ユーザホームネットワーク103内の各種のSAMが上述した機能を実現するために備える回路モジュールについて説明する。ユーザホームネットワーク103内のSAMとしては、前述したように、購入形態の決定などの権利処理（利益分配）に係わる処理を行うSAM105（105<sub>1</sub>～105<sub>4</sub>）と、記録媒体に設けられるメディアSAM133と、AV圧縮・伸長用SAM163と、メディア・ドラブSAM260とがある。以下、これらのSAMに設けられる回路モジュールをそれぞれ説明する。

【0280】＜権利処理用のSAMの第1形態＞図68は、権利処理用のSAM105aの回路モジュールを説明するための図である。図68に示すように、SAM105aは、CPU1100、DMA1101、MMU1102、I/Oモジュール1103、マスクROM1104、不揮発性メモリ1105、作業用RAM1106、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108、ハッシュ関数モジュール1109、（真性）乱数発生器1110、リアルタイムクロックモジュール1111、外部バス1/F1112を有する耐タンパ性のハードウェア（Tamper Resistant H/W）（本発明の回路モジュール）である。ここで、CPU1100が本発明の演算処理回路に対応し、マスクROM1104、不揮発性メモリ1105および作業用RAM1106が本発明の記憶回路に対応し、共通鍵暗号モジュール1108が本発明の暗号処理回路に対応し、外部バス1/F1112が本発明の外部バスインターフェイスに対応している。また、後述する図64の内部バス1120、1

121が本発明の第1のバスに対応し、外部バス1123が本発明の第2のバスに対応している。また、内部バス1120が本発明の第3のバスに対応し、内部バス1121が本発明の第4のバスに対応している。また、外部バス1/F1112が本発明の第1のインターフェイス回路に対応し、バス1/F回路1116が本発明の第2のインターフェイス回路に対応している。また、内部バス1122が本発明の第5のバスに対応し、I/Oモジュールが本発明の第3のインターフェイス回路に対応し、バス1/F回路1117が本発明の第4のインターフェイス回路に対応している。

【0281】図30に示すSAM105<sub>1</sub>の機能モジュールと、図68に示す回路モジュールとの関係を簡単に説明する。CPU1100は、例えば、マスクROM1104および不揮発性メモリ1105に記憶されたプログラムを実行して、図30に示すCPU1100、課金処理部187および利用監視部186の機能を実現する。DMA1101は、CPU1100からの命令に応じて、図22に示すダウンロードメモリ167および図30に示す記憶部192に対してのアクセスを統括的に制御する。MMU1102は、図22に示すダウンロードメモリ167および図30に示す記憶部192のアドレス空間を管理する。I/Oモジュール1103は、例えば、図30に示すメディアSAM管理部197の一部の機能を実現する。マスクROM1104には、SAM105aの初期化プログラムやインテグリティチェック（Integrity Check）プログラムなどの改ざりしないプログラムおよびデータが製造時に記憶され、図30に示す記憶部192の一部の機能を実現する。不揮発性メモリ1105は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶し、図30に示す記憶部192の一部の機能を実現する。作業用RAM1106は、図30に示す作業用メモリ200に対応している。

【0282】公開鍵暗号モジュール1107は、図30に示す署名処理部189の機能の一部を実現し、例えば、公開鍵暗号方式を用いた、メディアSAM133等と間の相互認証、SAM105の署名データの作成、署名データ（EMDサービスセンタ102、コンテンツプロバイダ101、第2実施形態の場合にはサービスプロバイダ310の署名データ）の検証、データ量の少ないデータ（キーファイルKFなど）の転送を行う際の当該データの暗号化および復号、並びに、鍵共有を行う際に用いられる。公開鍵暗号モジュール1107は、回路モジュールとして実現してもよい（H/W IP Solution）、不揮発性メモリ1105に記憶した公開鍵暗号プログラムをCPU1100において実行して実現してもよい（S/W IP Solution）。

【0283】共通鍵暗号モジュール1108は、図30に示す署名処理部189、暗号化・復号部171、172、173の機能の一部を実現し、相互認証、相互認証

によって得た共通鍵であるセッション鍵データKSESを用いたデータの暗号化および復号を行う際に用いられる。共通鍵暗号方式は、公開鍵暗号方式に比べて高速処理が可能であり、例えば、コンテンツデータ(コンテンツファイルCF)などのデータ量が大きいデータを暗号化および復号する際に用いられる。共通鍵暗号モジュール1108は、回路モジュールとして実現してもよいし(H/W IPSolution)、不揮発性メモリ1105に記憶した共通鍵暗号プログラムをCPU1100において実行して実現してもよい(S/W IPSolution)。なお、相互認証は、公開鍵暗号モジュール1107による暗号・復号および共通鍵暗号モジュール1108による暗号・復号の何れか一方あるいは双方を採用する。また、共通鍵暗号モジュール1108は、コンテンツ鍵データKcをライセンス鍵データKDを用いて復号する。

【0284】ハッシュ関数モジュール1109は、図30に示す署名処理部189の機能の一部を実現し、署名データを作成する対象となるデータのハッシュ値を生成する際に用いられる。具体的には、ハッシュ関数モジュール1109は、コンテンツプロバイダ101およびEMDサービスセンタ102などの署名データや、図44に示すセキュアコンテナ104xのキーファイルKF1のハッシュ値HK1を検証する際に用いられる。ハッシュ関数モジュール1109は、回路モジュールとして実現してもよいし(H/W IPSolution)、不揮発性メモリ1105に記憶したハッシュ回路モジュールをCPU1100において実行して実現してもよい(S/W IPSolution)。

【0285】乱数発生器1110は、例えば、図30に示す相互認証部170の機能の一部を実現する。リアルタイムクロックモジュール1111は、リアルタイムの時刻を発生する。当該時刻は、例えば、有効期限付きのライセンス鍵データKDを選択する場合や、利用制御データ166によって示される有効期限の要件を満たされているか否かを判断する際に用いられる。外部バスI/F1112は、図30に示すコンテンツプロバイダ管理部180、ダウンロードメモリ管理部182およびEMDサービスセンタ管理部185の一部の機能を実現する。

【0286】図69は、SAM105a内のハードウェア構成を説明するための図である。図69において、図68に示したものと同一回路モジュールには、図68と同じ符号を付している。図69に示すように、SAM105a内では、SAM・CPUバス1120を介してCPU1100、マスクROM1104および不揮発性メモリ1105が接続されている。内部バス1121には、DMA1101が接続されている。内部バス1122には、I<sup>2</sup>C・インターフェイス1130、メディアSAM・インターフェイス1131、MS(Memory Stick)・インターフェイス1132およびICカード・インターフェイス1133が接続されている。メディアSA

M・インターフェイス1131は記録媒体130のメディアSAM133との間でデータ転送を行う。MS・インターフェイス1132はメモリスティック1140との間でデータ転送を行う。ICカード・インターフェイス1133はICカード1141との間でデータ転送を行う。

【0287】外部バス1123には、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108、ハッシュ関数モジュール1109、乱数発生器1110、リアルタイムクロック生成モジュール1111、外部バスI/F1112および外部メモリI/F1140が接続されている。外部バスI/F1112は、図63に示す外部メモリ201が接続される。外部メモリI/F1140は、図63に示すホストCPUバス1000に接続される。

【0288】SAM・CPUバス1120と内部バス1121とは、バス・インターフェイス116を介して接続されている。内部バス1122と内部バス1121とは、バス・インターフェイス117を介して接続されている。内部バス1121と外部バス1123とは、バス・インターフェイス115を介して接続されている。

【0289】バス・インターフェイス1115内には、SRAM1155およびSAMステータスレジスタ1156が設けられている。SRAM1155は、後述するように、SAMステータスレジスタ1156には、前述のように、第1のSAMステータスレジスタおよび第2のSAMステータスレジスタがある。第1のSAMステータスレジスタには、ホストCPU810<sub>1</sub>によって読み出される、SAM105<sub>1</sub>のステータス(状態)を示すフラグが設定される。第2のSAMステータスレジスタには、ホストCPU810<sub>1</sub>からタスク実行の依頼が出されているか否かのステータスをSAM105<sub>1</sub>の内部のCPUから読み込むフラグが設定される。

【0290】DMA1101は、CPU1100からの命令に応じて、内部バス1121を介した、マスクROM1104、不揮発性メモリ1105および作業用RAM1106に対してのアクセスを統括的に制御する。M MU1113は、マスクROM1104、不揮発性メモリ1105、作業用RAM1106、図63に示すダウンロードメモリ167のメモリ空間を管理する。アドレスデコーダ1114は、内部バス1121と外部バス1123との間でデータ転送を行う際に、アドレス変換を行う。また、書き込みロック制御回路1135は、CPU1100からのロック鍵データに基づいて、フラッシュROMに対してのデータの書き込みおよび消去をブロック単位で管理する。

【0291】次に、権利処理用のSAM105aのアドレス空間を説明する。図70は、権利処理用のSAM105aのアドレス空間を説明するための図である。図7

0に示すように、権利処理用のSAM105aのアドレス空間には、開始アドレスから順に、例えば、ブートプログラム、システムコンフィギュレーション、フラッシュROM、所定のプログラム、フラッシュROMのデバイスドライバ、不揮発性メモリのデバイスドライバ、図69に示す作業用RAM1106、所定のプログラム、作業用RAM1108、所定のプログラム、図69に示すSRAM1155、外部メモリ201、Key\_TOC/File\_System、SAM登録リスト、利用履歴データ108、図69に示す共通鍵暗号モジュール1108のレジスタ、図69に示す公開鍵暗号モジュール1107のレジスタ、図69に示すハッシュ関数モジュール1109のレジスタ、図69に示す乱数発生器1110のレジスタ、図69に示すリアルタイムクロックモジュール1111のレジスタ、現在時刻レジスタ、有効期限レジスタ、コントロールレジスタ、ICカードのインターフェイス、メディアSAMのインターフェイス、メモリスティックのインターフェイス、I<sup>2</sup>Cバスのインターフェイスに割り当てられている。

【0292】システムコンフィギュレーションに割り当てられたアドレス空間内には、図69に示すDMA1101およびSAMステータスレジスタ1156が割り当てられている。また、フラッシュROMに割り当てられたアドレス空間内には、メインルーチン（カーネル）、割り込みプログラム、当該割り込みプログラムによって呼び出されるサブルーチン、コマンド解析部（コマンドと割り込みプログラムの開始アドレスの対応表）、割り込みベクタテーブルが割り当てられている。図70に示すSAM105aのアドレス空間のうち、SAMステータスレジスタ1156およびSRAM1155は、ホストCPU810との共有メモリ空間として用いられる。

【0293】次に、図63に示すホストCPU810<sub>1</sub>のアドレス空間を説明する。図71は、図63に示すホストCPU810<sub>1</sub>のアドレス空間を説明するための図である。図71に示すように、ホストCPU810<sub>1</sub>のアドレス空間は、開始アドレスから順に、例えば、ブートプログラム、システムコンフィギュレーション、コードが記憶されるROM、データが記憶されるRAM、作業用RAM、図63に示すSAM105<sub>1</sub>との共有メモリ、図63に示すAV圧縮・伸長用SAM163との共有メモリ、図63に示すメディア・ドラブSAM260との共有メモリおよび外部デバイスが割り当てられている。図63に示すSAM105<sub>1</sub>との共有メモリには、図63に示すSRAM1155およびSAMステータスレジスタ1156が割り当てられている。

【0294】＜権利処理用のSAMの第2形態＞図72は、権利処理用のSAM105bの回路モジュールを説明するための図である。図72では、SAM105aの構成要素と同じものには、図69と同じ符号を付している。図72に示すように、SAM105bは、セキュア

メモリ105ba、ホストCPU810、耐タンパ性ソフトウェア1130、I/Oモジュール1103を用いて実現される。SAM105bでは、ホストCPU810において、耐タンパ性ソフトウェア1130を実行することで、図68に示すCPU1100と同じ機能を実現する。耐タンパ性ソフトウェア1130は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解説および書き換え困難なソフトウェアである。セキュアメモリ105baには、マスクROM1104、不揮発性メモリ1105、作業用RAM1106、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108、ハッシュ関数モジュール1109、（真性）乱数発生器1110、リアルタイムクロックモジュール1111および外部バスI/F1112を有する耐タンパ性のハードウェアである。なお、公開鍵暗号モジュール1107、共通鍵暗号モジュール1108およびハッシュ関数モジュール1109は、回路モジュールとして実現してもよい（H/W IP Solution）、それぞれ不揮発性メモリ1105に記憶した公開鍵暗号プログラム、共通鍵暗号プログラムおよびハッシュ関数プログラムをホストCPU810において実行して実現してもよい（S/W IP Solution）。

【0295】以下、前述したメディアSAM133の構成の一例を説明する。図73は、メディアSAM133の回路モジュールを説明するための図である。図73に示すように、メディアSAM133は、CPU1200、DMA1201、I/Oモジュール1203、マスクROM1204、不揮発性メモリ1205、作業用RAM1206、公開鍵暗号モジュール1207、共通鍵暗号モジュール1208、ハッシュ関数モジュール1209、（真性）乱数発生器1210を有する耐タンパ性のハードウェア（Tamper Resistant H/W）である。

【0296】CPU1200は、耐タンパ性のハードウェア内の各回路の制御を行う。

【0297】作業用RAM1206は、図30に示す作業用メモリ200に対応している。公開鍵暗号モジュール1207は、例えば、公開鍵暗号方式を用いた、例えば（1）：図63に示すSAM105<sub>1</sub>およびドライバCPU1003等と間の相互認証、（2）メディアSAM133の署名データの作成、署名データ（EMDサブセンタ102、コンテンツプロバイダ101、第2実施形態の場合にはサブセンタプロバイダ310の署名データ）の検証、（3）：転送されるデータ量の少ないメッセージの暗号化および復号、並びに、（4）：相互認証によって得たセッション鍵データK<sub>SES</sub>の鍵共有を行う際に用いられる。公開鍵暗号モジュール1107は、回路モジュールとして実現してもよい（H/W IP Solution）、不揮発性メモリ1205に記憶した公開鍵暗号プログラムをCPU1200において実行して実現してもよい（S/W IP Solution）。



【0298】共通鍵暗号モジュール1208は、相互認証、相互認証によって得た共通鍵であるセッション鍵データK<sub>SES</sub>を用いたキーファイルKF、KF<sub>1</sub>などのデータの暗号化および復号を行う際に用いられる。共通鍵暗号モジュール1208は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1205に記憶した共通鍵暗号プログラムをCPU1200において実行して実現してもよい(S/W IP Solution)。なお、相互認証は、公開鍵暗号モジュール1207による暗号・復号および共通鍵暗号モジュール1208による暗号・復号の何れか一方あるいは双方を採用する。

【0299】ハッシュ関数モジュール1209は、データのハッシュ値を生成する際に用いられる。具体的には、ハッシュ関数モジュール1209は、図44に示すセキュアコンテナ104xのキーファイルKF<sub>1</sub>のハッシュ値H<sub>K1</sub>を検証する際に用いられる。ハッシュ関数モジュール1209は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1205に記憶したハッシュ回路モジュールをCPU1200において実行して実現してもよい(S/W IP Solution)。

【0300】乱数発生器1210は、例えば、相互認証を行う際に用いられる。1/0モジュール1203は、図63に示すメディアSAM1/F1007との間の通信を行う際に用いられる。

【0301】マスクROM1204には、メディアSAM133の初期化プログラムやインテグリティチェック(Integrity Check)プログラムなどの改変しないプログラムおよびデータが製造時に記憶される。不揮発性メモリ1205は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。

【0302】図74は、メディアSAM133がROM型の記録媒体に搭載される場合に、メディアSAM133の出荷時にマスクROM1204および不揮発性メモリ1205に格納されているデータを示す図である。図74に示すように、ROM型の記録媒体の出荷時には、メディアSAM133には、メディアSAMの識別子

(ID)、記録用鍵データK<sub>STR</sub>(メディア鍵データK<sub>MED</sub>)、EMDサービスセンタ102の公開鍵データK<sub>ESC</sub>、P、ルート認証局92の公開鍵データK<sub>R-CA</sub>、P、メディアSAM133の公開鍵証明書データCER<sub>MSAM</sub>、メディアSAM133の公開鍵データK<sub>MSAM</sub>、P、メディアSAM133の秘密鍵データK<sub>MSAM</sub>、S、リボケーションリスト、権利処理用データ、利益分配したいエンティティの識別子(ID)、メディアのタイプ(メディアの種別情報、ROMおよびRAMの何れかを特定する情報)、キーファイルKFの物理アドレス情報(レジスタ空間のアドレス)、各コンテンツデータC(コンテンツファイルCF)のキーファイルKF、所定の検証値(MAC値)などが記憶される。ここで、キーファイルKFの物理アドレス情報(レジスタ空間のアドレス)、各

コンテンツデータC(コンテンツファイルCF)のキーファイルKF、並びに所定の検証値(MAC値)は、EMDサービスセンタ102が管理するライセンス鍵データKDを用いて暗号化されている。

【0303】図75は、メディアSAM133がROM型の記録媒体に搭載される場合に、メディアSAM133の出荷後のユーザ登録およびコンテンツデータの購入形態決定処理を行ったときにマスクROM1204および不揮発性メモリ1205に格納されているデータを示す図である。図75に示すように、メディアSAM133には、ユーザ登録によって、新たに、ユーザID、パスワード、個人嗜好情報、個人決済情報(クレジットカード番号など)および電子マネー情報、キーファイルKF<sub>1</sub>などのデータが書き込まれる。

【0304】図76は、メディアSAM133がRAM型の記録媒体に搭載される場合に、メディアSAM133の出荷時にマスクROM1204および不揮発性メモリ1205に格納されているデータを示す図である。図76に示すように、RAM型の記録媒体の出荷時には、メディアSAM133には、メディアSAMの識別子(ID)、記録用鍵データK<sub>STR</sub>(メディア鍵データK<sub>MED</sub>)、EMDサービスセンタ102の公開鍵データK<sub>ESC</sub>、P、ルート認証局92の公開鍵データK<sub>R-CA</sub>、P、メディアSAM133の公開鍵証明書データCER<sub>MSAM</sub>、メディアSAM133の公開鍵データK<sub>MSAM</sub>、P、メディアSAM133の秘密鍵データK<sub>MSAM</sub>、S、リボケーションリスト、権利処理用データ、利益分配したいエンティティの識別子(ID)、メディアのタイプ(メディアの種別情報、ROMおよびRAMの何れかを特定する情報)が記憶されており、キーファイルKFの物理アドレス情報(レジスタ空間のアドレス)、各コンテンツデータC(コンテンツファイルCF)のキーファイルKF、KF<sub>1</sub>、所定の検証値(MAC値)などは記憶されていない。

【0305】図77は、メディアSAM133がRAM型の記録媒体に搭載される場合に、メディアSAM133の出荷後のユーザ登録およびコンテンツデータの購入形態決定処理を行ったときにマスクROM1204および不揮発性メモリ1205に格納されているデータを示す図である。図77に示すように、メディアSAM133には、ユーザ登録によって、新たに、ユーザID、パスワード、個人嗜好情報、個人決済情報(クレジットカード番号など)および電子マネー情報などのデータに加えて、キーファイルKFの物理アドレス情報(レジスタ空間のアドレス)、各コンテンツデータC(コンテンツファイルCF)のキーファイルKF、KF<sub>1</sub>、並びに所定の検証値(MAC値)が書き込まれる。キーファイルKFの物理アドレス情報(レジスタ空間のアドレス)、各コンテンツデータC(コンテンツファイルCF)のキーファイルKF、KF<sub>1</sub>、並びに所定の検証値(MAC

値)は、記録用鍵データKSTRによって暗号化されている。

【0306】<AV圧縮・伸長用SAM163>AV圧縮・伸長用SAM163は、例えば、図22を用いて説明した機能を実現する。図78は、AV圧縮・伸長用SAM163の回路モジュールを説明するための図である。図78に示すように、AV圧縮・伸長用SAM163は、CPU/DSP1300、DMA1301、マスクROM1304、不揮発性メモリ1305、作業用RAM1306、共通鍵暗号モジュール1308、(真性)乱数発生器1310、圧縮・伸長モジュール1320、電子透かし情報付加・検出モジュール1321および情報半開閉制御モジュール1322を有する耐タンパ性のハードウェア(Tamper Resistant H/W)である。

【0307】CPU/DSP1300は、例えば、図63に示すSAM105<sub>1</sub>からの命令に応じて、マスクROM1304および不揮発性メモリ1305に記憶されたプログラムを実行し、AV圧縮・伸長用SAM163内の各回路モジュールを統括的に制御する。DMA1301は、CPU/DSP1300からの命令に応じて、マスクROM1304、不揮発性メモリ1305、作業用RAM1306に対してのアクセスを統括的に制御する。マスクROM1304には、AV圧縮・伸長用SAM163の初期化プログラムやインテグリティチェック(Integrity Check)プログラムなどの改変しないプログラムや、AV圧縮・伸長用SAM163の識別子であるAVSAM\_IDなどの改変しないデータが製造時に記憶される。不揮発性メモリ1305は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。作業用RAM1306は、SAM105<sub>1</sub>から入力したキーファイルKFなどを記憶する。

【0308】共通鍵暗号モジュール1308は、SAM105<sub>1</sub>との間の相互認証、相互認証によって得た共通鍵であるセッション鍵データKSESを用いたコンテンツデータおよびコンテンツ鍵データKcなどの暗号化および復号を行う際に用いられる。共通鍵暗号モジュール1308は、回路モジュールとして実現してもよい(H/W IP Solution)、不揮発性メモリ1305に記憶した共通鍵暗号プログラムをCPU/DSP1300において実行して実現してもよい(S/W IP Solution)。また、共通鍵暗号モジュール1308は、SAM105<sub>1</sub>から得たコンテンツ鍵データKcを用いて、コンテンツデータCの復号を行う。乱数発生器1310は、例えば、SAM105<sub>1</sub>との間の相互認証処理を行う際に用いられる。

【0309】圧縮・伸長モジュール1320は、例えば、図22に示す伸長部223の機能を実現し、図63に示すダウンロードメモリ167およびショックブルーメモリ1004から入力したコンテンツデータの伸長処理と、A/D変換器から入力したコンテンツデータの

圧縮処理とを行う。

【0310】電子透かし情報添付・検出モジュール1321は、図22に示す電子透かし情報処理部224の機能を実現し、例えば、圧縮・伸長モジュール1320の処理対象となるコンテンツデータに対して所定の電子透かし情報を埋め込むと共に、当該コンテンツデータに埋め込まれた電子透かし情報を検出し、圧縮・伸長モジュール1320による処理の適否を判断する。

【0311】情報半開閉制御モジュール1322は、図22に示す半開閉処理部225の機能を実現し、必要に応じて、コンテンツデータを半開閉状態で再生する。

【0312】<メディア・ドラブSAM260>図79は、メディア・ドラブSAM260の回路モジュールを説明するための図である。図79に示すように、メディア・ドラブSAM260は、CPU1400、DMA1401、マスクROM1404、不揮発性メモリ1405、作業用RAM1406、共通鍵暗号モジュール1408、ハッシュ関数モジュール1409、(真性)乱数発生器1410、エンコーダ・デコーダモジュール1420、記録用鍵データ生成モジュール1430およびメディア・ユニークID生成モジュール1440を有する耐タンパ性のハードウェア(Tamper Resistant H/W)である。

【0313】CPU1400は、例えば、図63に示すドライブCPU1003からの命令に応じて、マスクROM1404および不揮発性メモリ1405に記憶されたプログラムを実行し、メディア・ドラブSAM260内の各回路モジュールを統括的に制御する。DMA1401は、CPU1400からの命令に応じて、マスクROM1404、不揮発性メモリ1405、作業用RAM1406に対してのアクセスを統括的に制御する。マスクROM1404には、メディア・ドラブSAM260の初期化プログラムやインテグリティチェック(Integrity Check)プログラムなどの改変しないプログラムや、メディア・ドラブSAM260の識別子であるMDSAM\_IDなどの改変しないデータが製造時に記憶される。不揮発性メモリ1405は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。作業用RAM1406は、種々の処理を行う際の作業用メモリとして用いられる。

【0314】共通鍵暗号モジュール1408は、メディアSAM133およびAV圧縮・伸長用SAM163との間の相互認証、相互認証によって得た共通鍵であるセッション鍵データKSESを用いたコンテンツファイルCFおよびキーファイルKFなどの暗号化および復号、並びに記録用鍵データKSTRおよびメディア鍵データKMEDを用いたコンテンツ鍵データKcの暗号化などを行う際に用いられる。また、共通鍵暗号モジュール1408は、共通鍵データと署名の対象となるデータのハッシュ値を用いて、署名データの検証および作成を行う。共

通鍵暗号モジュール1408は、回路モジュールとして実現してもよい(H/W IPSolution)、不揮発性メモリ1405に記憶した共通鍵暗号プログラムをCPU1400において実行して実現してもよい(S/W IPSolution)。なお、記録用鍵データKSTRを用いたコンテンツ鍵データKcの暗号化は、メディア・ドラッグSAM260の共通鍵暗号モジュール1408およびメディアSAM133の何れで行ってもよい。ハッシュ関数モジュール1409は、署名データの検証、並びに署名データを作成する対象となるデータのハッシュ値を生成する際に用いられる。乱数発生器1410は、例えば、メディアSAM133との間の相互認証処理を行う際に用いられる。

【0315】エンコーダ・デコーダモジュール1420は、記録媒体130のROM領域あるいはRAM領域に対して、コンテンツデータのアクセスを行う際に、当該コンテンツデータのエンコード処理、デコード処理、ECC(Error Correction Code)処理、変調処理、復調処理、セクタライズ処理およびデセクタライズ処理などを行う。

【0316】記録用鍵データ生成モジュール1430は、メディア・ユニークID生成モジュール1440が生成したメディア・ユニークIDを用いて、各メディアにユニークな記録用鍵データKSTRを生成する。

【0317】メディア・ユニークID生成モジュール1440は、メディア・ドラッグSAM260で生成したドライブIDと、メディアSAM133のメディアSAM\_IDとから、各記録媒体(メディア)にユニークなメディア・ユニークIDを生成する。

【0318】以下、図1に示すEMDシステム100の全体動作について説明する。図80は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1: EMDサービスセンタ102は、コンテンツプロバイダ101が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データKcp、pの公開鍵証明書CERcpをコンテンツプロバイダ101に送信する。また、EMDサービスセンタ102は、SAM1051~1054が所定の登録処理を経た後に、SAM1051~1054の公開鍵データKSAM1、p~KSAM4、pの公開鍵証明書CERCP1~CERCP4をSAM1051~1054に送信する。また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限が1カ月の3カ月のライセンス鍵データKD1~KD3をユーザホームネットワーク103のSAM1051~1054に送信する。このように、EMDシステム100では、ライセンス鍵データKD1~KD3を予めSAM1051~1054に配給しているため、SAM1051~1054とEMDサービスセンタ102との間がオフラインの状態でも、SAM1051~1054においてコンテンツプロバイダ101から配給されたセキュアコ

ンテナ104を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記述され、利用履歴データ108は、SAM1051~1054とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内、利用履歴データ108を回収できないSAM1について、リポケーションリストで無効の対象とする。なお、利用制御状態データ166は、原則として、リアルタイムで、SAM1051~1054からEMDサービスセンタ102に送信される。

【0319】ステップS2: コンテンツプロバイダ101は、EMDサービスセンタ102との間で相互認証を行った後に、権利書データ106およびコンテンツ鍵データKcをEMDサービスセンタ102に登録して権威化する。また、EMDサービスセンタ102は、6カ月分のキーファイルKFを作成し、これをコンテンツプロバイダ101に送信する。

【0320】ステップS3: コンテンツプロバイダ101は、図3(A)、(B)に示すコンテンツファイルCFおよびその署名データSIG6、cpと、キーファイルKFおよびその署名データSIG7、cpとを作成し、これらと図3(C)に示す公開鍵証明書CERcpおよびその署名データSIG1、ESCとを格納したセキュアコンテナ104を、オンラインおよび/またはオフラインで、ユーザホームネットワーク103のSAM1051~1054に配給する。オンラインの場合には、コンテンツプロバイダ101が用いた配送プロトコルを用いられ、当該プロトコルに依存しない形式で(すなわち、複数階層からなる通信プロトコルの所定の層を用いて伝送されるデータとして)、セキュアコンテナ104がコンテンツプロバイダ101からユーザホームネットワーク103に配送される。また、オフラインの場合には、ROM型あるいはRAM型の記録媒体に記録された状態で、セキュアコンテナ104が、コンテンツプロバイダ101からユーザホームネットワーク103に配送される。

【0321】ステップS4: ユーザホームネットワーク103のSAM1051~1054は、コンテンツプロバイダ101から配給を受けたセキュアコンテナ104内の署名データSIG6、cp、SIG7、cp、SIGK1、ESCを検証して、コンテンツファイルCFおよびキーファイルKFの作成者および送信者の正当性を確認した後に、対応する期間のライセンス鍵データKD1~KD6を用いてキーファイルKFを復号する。

【0322】ステップS5: SAM1051~SAM1054において、ユーザによる図2に示す操作部165の操作に応じたホストCPU810からの内部割り込みS810に基づいて、購入・利用形態を決定する。このとき、図37に示す利用監視部186において、セキ

ユーコンテナ104に格納された権利書データ106に基づいて、ユーザによるコンテンツファイルCの購入・利用形態が管理される。

【0323】ステップS6：SAM105<sub>1</sub>～SAM105<sub>4</sub>の図37に示す課金処理部187において、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ108および利用制御状態データ166が生成し、これらをEMDサービスセンタ102に送信する。

【0324】ステップS7：EMDサービスセンタ102は、利用履歴データ108に基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を作成する。EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG<sub>99</sub>を、図1に示すペイメントゲートウェイ9を介して、決済機関91に送信する。また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0325】ステップS8：決済機関91において、署名データSIG<sub>99</sub>の検証を行った後に、決済請求権データ152に基づいて、ユーザが支払った金額が、コンテンツプロバイダ101の所有者に分配される。

【0326】以上説明したように、EMDシステム100では、図3に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ101からユーザホームネットワーク103に配給し、セキュアコンテナ104内のキーファイルKFについての処理をSAM105<sub>1</sub>～105<sub>4</sub>内で行う。また、キーファイルKFに格納されたコンテンツ鍵データK<sub>c</sub>および権利書データ106は、配信鍵データKD<sub>1</sub>～KD<sub>3</sub>を用いて暗号化されており、配信鍵データKD<sub>1</sub>～KD<sub>3</sub>を保持しているSAM105<sub>1</sub>～105<sub>4</sub>内でのみ復号される。そして、SAM105<sub>1</sub>～105<sub>4</sub>では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。従って、EMDシステム100によれば、ユーザホームネットワーク103におけるコンテンツデータCの購入および利用を、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実にに行わせることができる。

【0327】また、EMDシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ104を用いて行うことで、SAM105<sub>1</sub>～105<sub>4</sub>におけるコンテンツデータCの権利処理を双方の場合において共通化できる。

【0328】また、EMDシステム100では、ユーザホームネットワーク103内のネットワーク機器160<sub>1</sub>およびAV機器160<sub>2</sub>～160<sub>4</sub>においてコンテ

ンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【0329】図8は、第1実施形態で採用されるセキュアコンテナの配送プロトコルの一例を説明するための図である。図81に示すように、マルチプロセスシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を配送するプロトコルとして例えばTCP/IPおよびXML/SMILが用いられる。また、ユーザホームネットワーク103のSAM相互間でセキュアコンテナを転送するプロトコル、並びにユーザホームネットワーク103と103aとの間でセキュアコンテナを転送するプロトコルとして例えば1394シリアルバス・インタフェース上に構築されたXML/SMILが用いられる。また、この場合に、ROM型やRAM型の記録媒体にセキュアコンテナを記録してSAM相互間で配送してもよい。

# 【0330】第2実施形態

上述した実施形態では、コンテンツプロバイダ101からユーザホームネットワーク103のSAM105<sub>1</sub>～105<sub>4</sub>にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのSAMに配給する場合について説明する。

【0331】図82は、本実施形態のEMDシステム300の構成図である。図82に示すように、EMDシステム300は、コンテンツプロバイダ301、EMDサービスセンタ302、ユーザホームネットワーク303、サービスプロバイダ310、ペイメントゲートウェイ90および決済機関91を有する。コンテンツプロバイダ301、EMDサービスセンタ302、SAM305<sub>1</sub>～305<sub>4</sub>およびサービスプロバイダ310は、それぞれ本発明のデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。コンテンツプロバイダ301は、サービスプロバイダ310に対してコンテンツデータを供給する点を除いて、前述した第1実施形態のコンテンツプロバイダ101と同じである。また、EMDサービスセンタ302は、コンテンツプロバイダ101およびSAM505<sub>1</sub>～505<sub>4</sub>に加えて、サービスプロバイダ310に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第1実施形態のEMDサービスセンタ102と同じである。また、ユーザホームネットワーク303は、ネットワーク機器360<sub>1</sub>およびAV機器360<sub>2</sub>～360<sub>4</sub>を有している。ネットワーク機器360<sub>1</sub>はSAM305<sub>1</sub>およびCAモジュール311を内蔵しており、AV機器360<sub>2</sub>～360<sub>4</sub>はそれぞれSAM305<sub>2</sub>～305<sub>4</sub>を内蔵している。ここで、SAM3

05<sub>1</sub>～305<sub>4</sub>は、サービスプロバイダ310からセキュアコンテナ304の配給を受ける点と、コンテンツプロバイダ301に加えてサービスプロバイダ310についての署名データの検証処理およびSP用購入履歴データ（データ配給装置用購入履歴データ）309の作成を行なう点とを除いて、前述した第1実施形態のSAM105<sub>1</sub>～105<sub>4</sub>と同じである。

【0332】 先ず、EMDシステム300の概要について説明する。EMDシステム300では、コンテンツプロバイダ301は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す前述した第1実施形態と同様の権利書(UCP: Usage Control Policy)データ106およびコンテンツ鍵データKcを、高い信頼性のある権威機関であるEMDサービスセンタ302に送信する。権利書データ106およびコンテンツ鍵データKcは、EMDサービスセンタ302に登録されて権威化（認証）される。

【0333】 また、コンテンツプロバイダ301は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から、各コンテンツファイルCFについて、それぞれ6か月分のキーファイルKFを受信する。当該キーファイルKF内には、当該キーファイルKFの改竄の有無、当該キーファイルKFの作成者および送信者の正当性を検証するための署名データが格納されている。そして、コンテンツプロバイダ301は、コンテンツファイルCF、キーファイルKFおよび自らの署名データとを格納した図3に示すセキュアコンテナ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いてあるいはオフラインなどでサービスプロバイダ310に供給する。また、セキュアコンテナ104に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【0334】 サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なって、セキュアコンテナ104の作成者および送信者の確認する。次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテンツプロバイダ301が希望するコンテンツに対しての価格（SRP）に、自らが行ったオーサリングなどのサービスに対しての価格を加算した価格を示すプライスタグデータ（PT：本発明の価格データ）312を作成する。そして、サービスプロバイダ310は、セキュアコンテナ104から取り出したコンテンツファイルCFおよびキーファイルKFと、プライスタグデータ312と、これらに対しての自らの秘密鍵データK<sub>Sp</sub>、S<sub>1</sub>による署名データとを格納したセキュアコンテナ304を作成する。このとき、キーファイルKFは、ライセンス

鍵データKD<sub>1</sub>～KD<sub>6</sub>によって暗号化されており、サービスプロバイダ310は当該ライセンス鍵データKD<sub>1</sub>～KD<sub>6</sub>を保持していないため、サービスプロバイダ310はキーファイルKFの中身を見たり、書き換えたりすることはできない。また、EMDサービスセンタ302は、プライスタグデータ312を登録して権威化する。

【0335】 サービスプロバイダ310は、オンラインおよび/またはオフラインでセキュアコンテナ304をユーザホームネットワーク303に配給する。このとき、オフラインの場合には、セキュアコンテナ304はROM型の記録媒体などに記録されてSAM305<sub>1</sub>～305<sub>4</sub>にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ310とCAモジュール311との間で相互認証を行い、セキュアコンテナ304をサービスプロバイダ310においてセッション鍵データK<sub>SES</sub>を用いた暗号化して送信し、CAモジュール311において受信したセキュアコンテナ304をセッション鍵データK<sub>SES</sub>を用いて復号した後に、SAM305<sub>1</sub>～305<sub>4</sub>に転送する。この場合に、コンテンツプロバイダ301からユーザホームネットワーク303にセキュアコンテナ304を送信する通信プロトコルとして、デジタル放送であればMPEG (Multimedia and Hy permedia information coding Experts Group)プロトコルが用いられ、インターネットであればXML/SMIL/HTML (Hyper Text Markup Language) が用いられ、これらの通信プロトコル内、セキュアコンテナ304が、当該通信プロトコル（符号化方式など）に依存しない形式でトンネリングして埋め込まれる。従って、通信プロトコルとセキュアコンテナ304との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ304のフォーマットを柔軟に設定できる。

【0336】 次に、SAM305<sub>1</sub>～305<sub>4</sub>において、セキュアコンテナ304内に格納された署名データを検証して、セキュアコンテナ304に格納されたコンテンツファイルCFおよびキーファイルKFの作成者および送信者の正当性を確認する。そして、SAM305<sub>1</sub>～305<sub>4</sub>において、当該正当性が確認されると、EMDサービスセンタ302から配給された対応する期間のライセンス鍵データKD<sub>1</sub>～KD<sub>3</sub>を用いてキーファイルKFを復号する。SAM305<sub>1</sub>～305<sub>4</sub>に供給されたセキュアコンテナ304は、ネットワーク機器360<sub>1</sub>およびAV機器360<sub>2</sub>～360<sub>4</sub>において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。SAM305<sub>1</sub>～305<sub>4</sub>は、上述したセキュアコンテナ304の購入・利用の履歴を利用履歴(Usage Log)データ308として記録する。利用履歴データ（履歴データまたは管理装置用履歴データ）308は、例えば、EMDサービスセンタ302からの要求に応じて、ユーザホームネッ

トワーク303からEMDサービスセンタ302に送信される。また、SAM3051～3054は、コンテンツの購入形態が決定されると、当該購入形態を示す利用制御データ(UCS:Usage control state Data)166をEMDサービスセンタ302に送信する。

【0337】EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101およびサービスプロバイダ310に分配される。

【0338】本実施形態では、EMDサービスセンタ302は、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有している。すなわち、EMDサービスセンタ302は、中立の立場にある最高の構成機関であるルート認証局92に対してのセカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ301、サービスプロバイダ310およびSAM3051～3054において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ302の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ301の権利書データ106、コンテンツ鍵データKcおよびサービスプロバイダ310のブライスタグデータ312を登録して権威化することも、EMDサービスセンタ302の認証機能によるものである。また、EMDサービスセンタ302は、例えば、ライセンス鍵データKD1～KD6などの鍵データの管理を行なう鍵データ管理機能を有する。また、EMDサービスセンタ302は、コンテンツプロバイダ301が登録した権利書データ106とSAM3051～SAM3054から入力した利用履歴データ308とサービスプロバイダ310が登録したブライスタグデータ312とに基づいて、ユーザホームネットワーク303のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ301およびサービスプロバイダ310に分配して支払う権利処理(利益分配)機能を有する。

【0339】以下、コンテンツプロバイダ301の各構成要素について詳細に説明する。

【コンテンツプロバイダ301】コンテンツプロバイダ301は、図3に示すセキュアコンテナ104をオンラインあるいはオフラインでサービスプロバイダ310に提供する点を除いて、前述した第1実施形態のコンテンツプロバイダ101と同じである。すなわち、コンテ

ツプロバイダ301は、前述した図17～図19に示す手順でセキュアコンテナ104を作成し、セキュアコンテナ104を、コンテンツプロバイダ用商品配送プロトコルに挿入する。そして、サービスプロバイダ310が、ダウンロードを行って、コンテンツプロバイダ用商品配送プロトコルからセキュアコンテナ104を取り出す。

【0340】【サービスプロバイダ310】サービスプロバイダ310は、コンテンツプロバイダ301から提供を受けたセキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFと、自らが生成したブライスタグデータ312とを格納したセキュアコンテナ304を作成し、ユーザホームネットワーク303のネットワーク機器3601およびAV機器3602～3604にセキュアコンテナ304をオンラインおよび/またはオフラインで配給する。サービスプロバイダ310によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、CM(広告)に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【0341】サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104の提供を受けると、以下に示す処理を行ってセキュアコンテナ304を作成する。以下、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104からセキュアコンテナ304を作成し、これをユーザホームネットワーク303に配給する際のサービスプロバイダ310内での処理の流れを図8を参照しながら説明する。図8は、サービスプロバイダ310からユーザホームネットワーク303にセキュアコンテナ304を配給する処理を説明するためのフローチャートである。

＜ステップS83-1＞サービスプロバイダ310は、オンラインおよび/またはオフラインで、コンテンツプロバイダ301から図3に示すセキュアコンテナ104の供給を受け、これを格納する。このとき、オンラインの場合には、コンテンツプロバイダ301とサービスプロバイダ310との間の相互認証によって得られたセッション鍵データKSESを用いて、セキュアコンテナ104を復号する。

＜ステップS83-2＞サービスプロバイダ310は、セキュアコンテナ104の図3(C)に示す署名データSIG1\_ESCを、EMDサービスセンタ302の公開鍵データKESC\_pを用いて検証し、その正当性が認められた後に、図3(C)に示す公開鍵証明書データCERT\_p

から公開鍵データ $K_{CP}$ を取り出す。次に、サービスプロバイダ310は、当該取り出した公開鍵データ $K_{CP}$ を用いて、セキュアコンテナ104の図3(A)、

(B)に示す署名データ $SIG_6, CP$ 、 $SIG_7, CP$ の検証、すなわちコンテンツファイルCFの作成者および送信者と、キーファイルKFの送信者との正当性の検証を行う。また、サービスプロバイダ310は、公開鍵データ $K_{ESC, P}$ を用いて、図3(B)に示すキーファイルKFに格納された署名データ $SIG_{K1, ESC}$ の検証、すなわちキーファイルKFの作成者の正当性の検証を行う。このとき、署名データ $SIG_{K1, ESC}$ の検証は、キーファイルKFがEMDサービセンタ302に登録されているか否かの検証も兼ねている。

【0342】<ステップS83-3>サービスプロバイダ310は、例えばコンテンツプロバイダ301からオフラインで通知されたコンテンツプロバイダ301が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ312を作成する。また、サービスプロバイダ310は、コンテンツファイルCF、キーファイルKFおよびプライスタグデータ312のハッシュ値をとり、サービスプロバイダ310の秘密鍵データ $K_{SP}$ を用いて、署名データ $SIG_{G2, SP}$ 、 $SIG_{G3, SP}$ 、 $SIG_{G4, SP}$ を作成する。ここで、署名データ $SIG_{G2, SP}$ はコンテンツファイルCFの送信者の正当性を検証するために用いられ、署名データ $SIG_{G3, SP}$ はキーファイルKFの送信者の正当性を検証するために用いられ、署名データ $SIG_{G4, SP}$ はプライスタグデータ312の作成者および送信者の正当性を検証するために用いられる。

【0343】次に、サービスプロバイダ310は、図4(A)～(D)に示すように、コンテンツファイルCFおよびその署名データ $SIG_6, CP$ 、 $SIG_{G2, SP}$ と、キーファイルKFおよびその署名データ $SIG_7, CP$ 、 $SIG_{G3, ESC}$ と、プライスタグデータ312およびその署名データ $SIG_{G4, SP}$ と、公開鍵証明書データ $CER_{SP}$ およびその署名データ $SIG_{K1, ESC}$ と、公開鍵証明書データ $CER_{CP}$ およびその署名データ $SIG_{K1, ESC}$ とを格納したセキュアコンテナ304を作成し、セキュアコンテナデータベースに格納する。セキュアコンテナデータベースに格納されたセキュアコンテナ304は、例えば、コンテンツIDなどを用いてサービスプロバイダ310によって一元的に管理される。なお、図4(A)は、コンテンツデータCを伸長するAV圧縮伸長用装置として、DSP(Digital Signal Processor)を用いた場合のコンテンツファイルCFの構成である。当該DSPでは、セキュアコンテナ304内のA/V伸長用ソフトウェアおよび電子透かし情報モジュールを用いて、セキュアコンテナ104内のコンテンツデータCの伸長および電子透かし情報の埋め込みおよび検出を行う。そのため、コンテンツプロバイダ301は任意の圧縮方式およ

び電子透かし情報の埋め込み方式を採用できる。AV圧縮伸長用装置としてA/V伸長処理および電子透かし情報の埋め込み・検出処理をハードウェアあるいは予め保持されたソフトウェアを用いて行う場合には、コンテンツファイルCF内にA/V伸長用ソフトウェアおよび電子透かし情報モジュールを格納しなくてもよい。

【0344】<ステップS83-4>サービスプロバイダ310は、ユーザホームネットワーク303からの要求に応じたセキュアコンテナ304をセキュアコンテナデータベースから読み出す。このとき、セキュアコンテナ304は、複数のコンテンツファイルCFと、それらにそれぞれ対応した複数のキーファイルKFとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ304内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルCFを単数のセキュアコンテナ304に格納してもよい。これらの複数のコンテンツファイルCFなどは、ディレクトリ構造でセキュアコンテナ304内に格納してもよい。

【0345】また、セキュアコンテナ304は、デジタル放送で送信される場合には、MHEG(Multimedia and Hypermedia information coding Experts Group)プロトコルが用いられ、インターネットで送信される場合にはXML/SMIL/HTML(Hyper Text Markup Language)プロトコルが用いられる。このとき、セキュアコンテナ304内のコンテンツファイルCFおよびキーファイルKFなどは、MHEGおよびHTMLのプロトコルをトンネリングした符号化方式に依存しない形式で、サービスプロバイダ310とユーザホームネットワーク303との間で採用される通信プロトコル内の所定の階層に格納される。

【0346】例えば、セキュアコンテナ304をデジタル放送で送信する場合には、図85に示すように、コンテンツファイルCFが、MHEGオブジェクト(Object)内のMHEGコンテンツデータとして格納される。また、MHEGオブジェクトは、トランスポート層プロトコルにおいて、動画である場合にはPES(Packetized Elementary Stream)-Videoに格納され、音声である場合にはPES-Audioに格納され、静止画である場合にはPrivate-Dataに格納される。また、図86に示すように、キーファイルKF、プライスタグデータ312および公開鍵証明書データ $CER_{CP}$ 、 $CER_{SP}$ は、トランスポート層プロトコルのTS Packet内のECM(Entitlement Control Message)に格納される。ここで、コンテンツファイルCF、キーファイルKF、プライスタグデータ312および公開鍵証明書データ $CER_{CP}$ 、 $CER_{SP}$ は、コンテンツファイルCFのヘッダ内のディレクトリ構造データ $DSD_1$ によって相互間のリンクが確立されている。

【0347】次に、サービスプロバイダ310は、セキ

ユーコンテナ304を、オフラインおよび/またはオンラインでユーザホームネットワーク303に供給する。サービスプロバイダ310は、セキュアコンテナ304をオンラインでユーザホームネットワーク303のネットワーク機器360<sub>1</sub>に配信する場合には、相互認証後に、セッション鍵データK<sub>SES</sub>を用いてセキュアコンテナ304を暗号化した後に、ネットワークを介してネットワーク機器360<sub>1</sub>に配信する。

【0348】なお、サービスプロバイダ310は、セキュアコンテナ304を例えば衛星などを介して放送する場合にも、セキュアコンテナ304をスクランブル鍵データK<sub>SCR</sub>を用いて暗号化する。また、スクランブル鍵データK<sub>SCR</sub>をワーク鍵データK<sub>W</sub>を暗号化し、ワーク鍵データK<sub>W</sub>をマスク鍵データK<sub>M</sub>を用いて暗号化する。そして、サービスプロバイダ310は、セキュアコンテナ304と共に、スクランブル鍵データK<sub>SCR</sub>およびワーク鍵データK<sub>W</sub>を、衛星を介してユーザホームネットワーク303に送信する。また、例えば、マスク鍵データK<sub>M</sub>を、ICカードなどに記憶してオフラインでユーザホームネットワーク303に供給する。

【0349】また、サービスプロバイダ310は、ユーザホームネットワーク303から、当該サービスプロバイダ310が配給したコンテンツデータCに関してのSP用購入履歴データ309を受信すると、これを格納する。サービスプロバイダ310は、将来のサービス内容を決定する際に、SP用購入履歴データ309を参照する。また、サービスプロバイダ310は、SP用購入履歴データ309に基づいて、当該SP用購入履歴データ309を送信したSAM305<sub>1</sub>～305<sub>4</sub>のユーザの嗜好を分析してユーザ嗜好フィルタデータ900を生成し、これをユーザホームネットワーク303のCAモジュール311に送信する。

【0350】また、サービスプロバイダ310の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ302に登録処理を行い、グローバルユニークな識別子SP\_IDを得ている。

【0351】また、サービスプロバイダ310は、EMDサービスセンタ302にプライスタグデータ312を登録して権威化している。

【0352】[EMDサービスセンタ302] EMDサービスセンタ302は、前述したように、認証局(CA:Certificate Authority)、鍵管理(Key Management)局および権利処理(Rights Clearing)局としての役割を果たす。図87は、EMDサービスセンタ302の主な機能を示す図である。図87に示すように、EMDサービスセンタ302は、主に、ライセンス鍵データをコンテンツプロバイダ301およびSAM305<sub>1</sub>～305<sub>4</sub>に供給する処理と、公開鍵証明書データCERCP、CERSp、CERSAM1～CERSAM4の発行処理と、キー

ファイルKFの発行処理、利用履歴データ308に基づいた決済処理(利益分配処理)とを行う。ここで、ライセンス鍵データの供給処理と、公開鍵証明書データCERCP、CERSAM1～CERSAM4の発行処理と、キーファイルKFの生成処理とは、第1実施形態のEMDサービスセンタ102と同じである。

【0353】EMDサービスセンタ302は、EMDサービスセンタ102とは異なり、さらにサービスプロバイダ310の公開鍵証明書データCERSpの発行処理を行う。また、EMDサービスセンタ302は、利用履歴データ308に基づいて、SAM305<sub>1</sub>～305<sub>4</sub>におけるコンテンツデータCの購入によって支払われた利益をコンテンツプロバイダ301およびサービスプロバイダ310の関係者に分配する利益分配処理を行う。ここで、利用履歴データ308の内容は、例えば図21に示される。

【0354】また、EMDサービスセンタ302は、利用履歴データ308に基づいて、当該利用履歴データ308を送信したSAM305<sub>1</sub>～305<sub>4</sub>のユーザの嗜好に応じたコンテンツデータCを選択するためのユーザ嗜好フィルタデータ903を生成し、ユーザ嗜好フィルタデータ903をSAM管理部149を介して、当該利用履歴データ308を送信したSAM305<sub>1</sub>～305<sub>4</sub>に送信する。

【0355】[ユーザホームネットワーク303] ユーザホームネットワーク303は、図82に示すように、ネットワーク機器360<sub>1</sub>およびA/V機器360<sub>2</sub>～360<sub>4</sub>を有している。ネットワーク機器360<sub>1</sub>は、CAモジュール311およびSAM305<sub>1</sub>を内蔵している。また、AV機器360<sub>2</sub>～360<sub>4</sub>は、それぞれSAM305<sub>2</sub>～305<sub>4</sub>を内蔵している。SAM305<sub>1</sub>～305<sub>4</sub>の相互間は、例えば、1394シリアルインタフェースバスなどのバス191を介して接続されている。なお、AV機器360<sub>2</sub>～360<sub>4</sub>は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器360<sub>1</sub>のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク303は、ネットワーク機能を有していないAV機器のみを有していてもよい。

【0356】以下、ネットワーク機器360<sub>1</sub>について説明する。図88は、ネットワーク機器360<sub>1</sub>の構成図である。図88に示すように、ネットワーク機器360<sub>1</sub>は、通信モジュール162、CAモジュール311、復号モジュール905、SAM305<sub>1</sub>、AV圧縮・伸長用SAM163、操作部165、ダウンロードメモリ167、再生モジュール169、外部メモリ201およびホストCPU810を有する。図88において、図22と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。



【0357】通信モジュール162は、サービスプロバイダ310との間の通信処理を行なう。具体的には、通信モジュール162は、サービスプロバイダ310から衛星放送などを受信したセキュアコンテナ304を復号モジュール905に出力する。また、通信モジュール162は、サービスプロバイダ310から電話回線などを介して受信したユーザ嗜好フィルタデータ900をCAモジュール311に出力すると共に、CAモジュール311から入力したSP用購入履歴データ309を電話回線などを介してサービスプロバイダ310に送信する。

【0358】図89は、CAモジュール311および復号モジュール905の機能ブロック図である。図89に示すように、CAモジュール311は、相互認証部906、記憶部907、暗号化・復号部908およびSP用購入履歴データ生成部909を有する。相互認証部906は、CAモジュール311とサービスプロバイダ310との間で電話回線を介してデータを送受信する際に、サービスプロバイダ310との間で相互認証を行ってセッション鍵データK<sub>SES</sub>を生成し、これを暗号化・復号部908に出力する。

【0359】記憶部907は、例えば、サービスプロバイダ310とユーザとの間で契約が成立した後に、サービスプロバイダ310からICカード912などを介してオフラインで供給されたマスク鍵データK<sub>M</sub>を記憶する。

【0360】暗号化・復号部908は、復号モジュール905の復号部910からそれぞれ暗号化されたスクランブル鍵データK<sub>SCR</sub>およびワーク鍵データK<sub>W</sub>を入力し、記憶部907から読み出したマスク鍵データK<sub>M</sub>を用いてワーク鍵データK<sub>W</sub>を復号する。そして、暗号化・復号部908は、当該復号したワーク鍵データK<sub>W</sub>を用いてスクランブル鍵データK<sub>SCR</sub>を復号し、当該復号したスクランブル鍵データK<sub>SCR</sub>を復号部910に出力する。また、暗号化・復号部908は、電話回線などを介して通信モジュール162がサービスプロバイダ310から受信したユーザ嗜好フィルタデータ900を、相互認証部906からのセッション鍵データK<sub>SES</sub>を用いて復号して復号モジュール905のセキュアコンテナ選択部911に出力する。また、暗号化・復号部908は、SP用購入履歴データ生成部909から入力したSP用購入履歴データ309を、相互認証部906からのセッション鍵データK<sub>SES</sub>を用いて復号して通信モジュール162を介してサービスプロバイダ310に送信する。

【0361】SP用購入履歴データ生成部909は、図88に示す購入・利用形態決定操作部165を用いてユーザによるコンテンツデータの購入操作に応じた操作信号S165、またはSAM305<sub>1</sub>からの利用制御データ166に基づいて、サービスプロバイダ310に固有のコンテンツデータCの購入履歴を示すSP用購入履

歴データ309を生成し、これを暗号化・復号部908に出力する。SP用購入履歴データ309は、例えば、サービスプロバイダ310が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【0362】なお、CAモジュール311は、サービスプロバイダ310が課金機能を有している場合には、サービスプロバイダ310の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、CAモジュール311は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ310に送信する。

【0363】復号モジュール905は、復号部910およびセキュアコンテナ選択部911を有する。復号部910は、通信モジュール162から、それぞれ暗号化されたセキュアコンテナ304、スクランブル鍵データK<sub>SCR</sub>およびワーク鍵データK<sub>W</sub>を入力する。そして、復号部910は、暗号化されたスクランブル鍵データK<sub>SCR</sub>およびワーク鍵データK<sub>W</sub>をCAモジュール311の暗号化・復号部908に出力し、暗号化・復号部908から復号されたスクランブル鍵データK<sub>SCR</sub>を入力する。そして、復号部910は、暗号化されたセキュアコンテナ304を、スクランブル鍵データK<sub>SCR</sub>を用いて復号した後に、セキュアコンテナ選択部911に出力する。

【0364】なお、セキュアコンテナ304が、MPEG2 Transport Stream 方式でサービスプロバイダ310から送信される場合には、例えば、復号部910は、TS Packet 内のECM (Entitlement Control Message) からスクランブル鍵データK<sub>SCR</sub>を取り出し、EMM (Entitlement Management Message) からワーク鍵データK<sub>W</sub>を取り出す。ECMには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、EMMは、その他に、ユーザ（視聴者）毎に異なる個別視聴契約情報などが含まれている。

【0365】セキュアコンテナ選択部911は、復号部910から入力したセキュアコンテナ304を、CAモジュール311から入力したユーザ嗜好フィルタデータ900を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ304を選択してSAM305<sub>1</sub>に出力する。

【0366】次に、SAM305<sub>1</sub>について説明する。なお、SAM305<sub>1</sub>は、サービスプロバイダ310についての署名検証処理を行なうなど、コンテンツプロバイダ301に加えてサービスプロバイダ310に関しての処理を行う点を除いて、図22～図72などを用いて前述した第1実施形態のSAM105<sub>1</sub>と基本的に行なう機能および構造を有している。している。SAM305<sub>1</sub>～305<sub>4</sub>は、コンテンツ単位の課金処理を行うモ

ジュールであり、EMDサービスセンタ302との間で通信を行う。

【0367】また、図63に示す構成はユーザホームネットワーク303内の機器においても適用可能である。また、図68～図79を用いて説明した権利処理用のSAM、メディアSAM133、AV圧縮・伸長用SAM163およびメディア・ドラブSAM260の構成は、ユーザホームネットワーク303内の機器で用いられる各種のSAMにも適用される。また、SAM305<sub>2</sub>～305<sub>4</sub>は、SAM305<sub>1</sub>と基本的に同じ機能を有する。

【0368】以下、SAM305<sub>1</sub>の機能について詳細に説明する。図90は、SAM305<sub>1</sub>の機能の構成図である。なお、図90には、サービスプロバイダ310からセキュアコンテナ304を入力する際の処理に関連するデータの流れが示されている。図90に示すように、SAM305<sub>1</sub>は、相互認証部170、暗号化・復号部171、172、173、ダウンロードメモリ管理部182、AV圧縮・伸長用SAM管理部184、EMDサービスセンタ管理部185、利用履歴部186、SAM管理部190、記憶部192、メディアSAM管理部197、作業用メモリ200、サービスプロバイダ管理部580、課金処理部587、署名処理部589、外部メモリ管理部811およびCPU1100を有する。なお、図90に示すSAM305<sub>1</sub>の所定の機能は、SAM105<sub>1</sub>の場合と同様に、CPUにおいて秘密プログラムを実行することによって実現される。図90において、図30等と同じ符号を付した機能ブロックは、第1実施形態で説明した同一符号の機能ブロックと同じである。

【0369】また、図88に示す外部メモリ201には、第1実施形態で説明した処理および後述する処理を経て、利用履歴データ308およびSAM登録リストが記憶される。また、作業用メモリ200には、図91に示すように、コンテンツ鍵データK<sub>c</sub>、権利書データ(UCP)106、記憶部192のロック鍵データK<sub>L0C</sub>、コンテンツプロバイダ301の公開鍵証明書データCER<sub>CP</sub>、サービスプロバイダ310の公開鍵証明書データCER<sub>SP</sub>、利用制御データ(UCS)366、SAMプログラム・ダウンロード・コンテナSDC<sub>1</sub>～SDC<sub>3</sub>およびブライスタグデータ312などが記憶される。

【0370】以下、SAM305<sub>1</sub>の機能ブロックのうち、図90において新たに符号を付した機能ブロックについて説明する。署名処理部589は、記憶部192あるいは作業用メモリ200から読み出したEMDサービスセンタ302の公開鍵データK<sub>ESC</sub>、コンテンツプロバイダ301の公開鍵データK<sub>CP</sub>およびサービスプロバイダ310の公開鍵データK<sub>SP</sub>を用いて、セキュアコンテナ304内の署名データの検証を行なう。

【0371】課金処理部587は、図92に示すよう

に、ユーザによる購入形態決定操作に応じた内部割り込みS810をCPU1100がホストCPU810から受けると、CPU1100からの制御によって、作業用メモリ200から読み出されたブライスタグデータ312に基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。なお、ブライスタグデータ312は、ユーザがコンテンツデータの購入形態等を決定する際に、所定の出力手段を介してSAM305<sub>1</sub>の外部に出力され、コンテンツデータの販売価格をユーザに表示等するために用いられる。課金処理部587による課金処理は、利用履歴部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【0372】また、課金処理部587は、課金処理において、利用履歴データ308を生成あるいは更新し、これを外部メモリ管理部811を介して外部メモリ201に書き込む。ここで、利用履歴データ308は、第1実施形態の利用履歴データ108と同様に、EMDサービスセンタ302において、セキュアコンテナ304に関連したライセンス料の支払いを決定する際に用いられる。

【0373】また、課金処理部587は、ユーザによる購入形態決定操作に応じたCPU1100の制御に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御(UCS: Usage Control Status)データ166を生成し、これを作業用メモリ200に書き込む。コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御データ166には、コンテンツのID、購入形態、買い切り価格、当該コンテンツの購入が行なわれたSAMのSAM\_ID、購入を行なったユーザのUSER\_IDなどが記述されている。

【0374】なお、決定された購入形態が再生課金である場合には、例えば、SAM305<sub>1</sub>からサービスプロバイダ310に利用制御データ166をリアルタイムに送信し、サービスプロバイダ310がEMDサービスセンタ302に、利用履歴データ308をSAM105<sub>1</sub>に取りに行くことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御データ166が、サービスプロバイダ310およびEMDサービスセンタ302にリアルタイムに送信される。

【0375】また、SAM305<sub>1</sub>では、図90に示すように、EMDサービスセンタ管理部185を介してE

MDサービスセンタ302から受信したユーザ嗜好フィルタデータ903が、サービスプロバイダ管理部580に出力される。そして、サービスプロバイダ管理部580において、図88に示す番号モジュール905から入力したセキュアコンテナ304のうち、ユーザ嗜好フィルタデータ903に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ304が選択され、当該選択されたセキュアコンテナ304がダウンロードメモリ管理部182に出力される。これにより、SAM3051において、当該SAM3051のユーザが契約している全てのサービスプロバイダ310を対象として、当該ユーザによるコンテンツデータCの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータCの選択処理が可能になる。

【0376】以下、SAM3051内での処理の流れを説明する。

<ライセンス鍵データの受信時の処理> EMDサービスセンタ302から受信したライセンス鍵データKD1～KD3を記憶部192に格納する際のSAM3051内での処理の流れは、図35を用いて前述した第1実施形態のSAM1051の場合と同様である。

【0377】<セキュアコンテナ304をサービスプロバイダ310から入力した時の処理> 次に、セキュアコンテナ304をサービスプロバイダ310から入力する際のSAM3051内での処理の流れを図93を参照しながら説明する。なお、以下に示す例では、SAM1051において、セキュアコンテナ104を入力したときに種々の署名データの検証を行う場合を例示するが、セキュアコンテナ104の入力したときには当該署名データの検証を行わずに、購入・利用形態を決定するときに当該署名データの検証を行うようにしてもよい。

【0378】ステップS93-0：図90に示すSAM3051のCPU1100は、ホストCPU810から、セキュアコンテナの入力処理を行うことを指示する内部割り込みS810を受ける。

ステップS93-1：図90に示すSAM3051の相互認証部170とサービスプロバイダ310との間で相互認証を行う。

ステップS93-2：SAM3051の相互認証部170とダウンロードメモリ167のメディアSAM167aとの間で相互認証を行う。

【0379】ステップS93-3：サービスプロバイダ310から受信したセキュアコンテナ304を、ダウンロードメモリ167に書き込む。このとき、ステップS93-2で得られたセッション鍵データを用いて、相互認証部170におけるセキュアコンテナ304の暗号化と、メディアSAM167aにおけるセキュアコンテナ304の復号とを行なう。

ステップS93-4：SAM3051は、ステップS93-1で得られたセッション鍵データを用いて、セキュア

コンテナ304の復号を行なう。

【0380】ステップS93-5：署名処理部589は、図84(D)に示す署名データSIG61、ESCの検証を行なった後に、図84(D)に示す公開鍵証明書データCERSp内に格納されたサービスプロバイダ310の公開鍵データKSpを用いて、署名データSIG62、SP、SIG63、SP、SIG64、SPの正当性を検証する。このとき、署名データSIG62、SPが正当であると検証されたときに、コンテンツファイルCFの送信者の正当性が確認される。署名データSIG63、SPが正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。署名データSIG64、SPが正当であると検証されたときに、プライスタグデータ312の作成者および送信者の正当性が確認される。

【0381】ステップS93-6：署名処理部589は、図84(D)に示す署名データSIG1、ESCの検証を行なった後に、図84(C)に示す公開鍵証明書データCERSp内に格納されたコンテンツプロバイダ301の公開鍵データKCP、pを用いて、署名データSIG6、CP、SIG7、CPの正当性を検証する。このとき、署名データSIG6、CPが正当であると検証されたときに、コンテンツファイルCFの作成者および送信者の正当性が確認される。また、署名データSIG7、CPが正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

【0382】ステップS93-7：署名処理部589は、記憶部192から読み出した公開鍵データKESC、pを用いて、図84(B)に示すキーファイルKF内の署名データSIGK1、ESCの正当性、すなわちキーファイルKFの作成者の正当性およびキーファイルKFがEMDサービスセンタ102に登録されているか否かの検証を行う。

【0383】ステップS93-8：暗号化・復号部172は、記憶部192から読み出した対応する期間のライセンス鍵データKD1～KD3を用いて、図84(B)に示すキーファイルKF内のコンテンツ鍵データKc、権利書データ106およびSAMプログラム・ダウンロード・コンテナSDC1～SDC3を復号し、これらを作業用メモリ200に書き込む。

【0384】ステップS93-9：CPU1100は、上述したセキュアコンテナの入力処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。なお、CPU1100は、上述したセキュアコンテナの入力処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0385】<ダウンロードしたセキュアコンテナの購入形態決定処理> ダウンロードしたセキュアコンテナの購入形態決定処理は、基本的に、第1実施形態において、図38を用いて前述したSAM1051の場合と同

じである。当該購入形態決定処理により、後述する図97(C)に示すキーファイルKF<sub>1</sub>が作業用メモリ200およびダウンロードメモリ182を介してダウンロードメモリ167に記憶される。

【0386】<コンテンツデータの再生処理>ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCの再生処理は、基本的に、第1実施形態において、図40を用いて説明したSAM105<sub>1</sub>の処理と同じである。

【0387】<一の機器の利用制御データ(USC)166を使用して他の機器で再購入を行う場合の処理>先ず、図94に示すように、例えば、ネットワーク機器360<sub>1</sub>のダウンロードメモリ167にダウンロードされたコンテンツファイルCFの購入形態を前述したように決定した後に、当該コンテンツファイルCFを格納した新たなセキュアコンテナ304xを生成し、バス191を介して、AV機器360<sub>2</sub>のSAM305<sub>2</sub>にセキュアコンテナ304xを転送するまでのSAM105<sub>1</sub>内での処理の流れを図95および図96を参照しながら説明する。

【0388】図96は、当該処理のフローチャートである。図96に示す処理を行う前提として、前述した購入処理によって、SAM305<sub>1</sub>の作業用メモリ200には図97(C)に示すキーファイルKF<sub>1</sub>およびそのハッシュ値H<sub>K1</sub>が記憶されている。

ステップS96-1: ユーザは図88および図94に示すに操作部165を操作し、購入形態を既に決定したセキュアコンテナをSAM305<sub>2</sub>に転送することを示す内部割り込みS810がホストCPU810から図95に示すCPU1100に出される。課金処理部587は、CPU1100の制御に基づいて、決定された購入形態に応じて、外部メモリ201に記憶されている利用履歴データ308を更新する。

【0389】ステップS96-2: SAM305<sub>1</sub>は、第1実施形態で前述したSAM登録リストを検証し、セキュアコンテナの転送先のSAM305<sub>2</sub>が正規に登録されているSAMであるか否かを検証し、正規に登録されていると判断した場合にステップS96-3以降の処理を行う。また、SAM105<sub>1</sub>は、SAM105<sub>2</sub>がホームネットワーク内のSAMであるか否かの検証も行う。

【0390】ステップS96-3: 相互認証部170は、SAM305<sub>2</sub>との間で相互認証を行って得たセッション鍵データK<sub>SES</sub>を共有する。

【0391】ステップS96-4: SAM管理部190は、ダウンロードメモリ211から図84(A)に示すコンテンツファイルCFおよび署名データSIG<sub>6</sub>, CP, S1G62, SPを読み出し、これについてのSAM305<sub>1</sub>の秘密鍵データK<sub>SAM1</sub>を用いた署名データSIG41, SAM1を署名処理部589に作成させる。

【0392】ステップS96-5: SAM管理部190は、ダウンロードメモリ211から図84(B)に示すキーファイルKFおよび署名データSIG7, CP, S1G63, SPを読み出し、これについてのSAM305<sub>1</sub>の秘密鍵データK<sub>SAM1</sub>を用いた署名データSIG42, SAM1を署名処理部589に作成させる。

【0393】ステップS96-6: SAM管理部190は、図97に示すセキュアコンテナ304xを作成する。

ステップS96-7: 暗号化・復号部171において、ステップS96-3で得たセッション鍵データK<sub>SES</sub>を用いて、図97に示すセキュアコンテナ304xが暗号化される。

【0394】ステップS96-8: SAM管理部190は、セキュアコンテナ304xを図94に示すAV機器360<sub>2</sub>のSAM305<sub>2</sub>に出力する。このとき、SAM305<sub>1</sub>とSAM305<sub>2</sub>との間の相互認証と並行して、IEEE1394シリアルバスであるバス191の相互認証が行われる。

【0395】ステップS96-9: CPU1100は、上述したセキュアコンテナの転送処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。なお、CPU1100は、上述したセキュアコンテナの転送処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0396】以下、図94に示すように、SAM305<sub>1</sub>から入力した図97に示すセキュアコンテナ304xを、RAM型などの記録媒体(メディア)1304に書き込む際のRAM領域134、メディアSAM133およびセキュアRAM領域132を有している。

【0397】ステップS99-0: 図98に示すSAM305<sub>2</sub>のCPU1100は、ホストCPU810から、入力したセキュアコンテナを購入形態を決定した後記録媒体に記録することを指示する内部割り込みS810を受ける。

【0398】ステップS99-1: SAM305<sub>2</sub>は、SAM登録リストを検証し、セキュアコンテナの転送元のSAM305<sub>1</sub>が正規に登録されているSAMであるか否かを検証し、正規に登録されていると判断した場合にステップS99-2以降の処理を行う。また、SAM305<sub>2</sub>は、SAM305<sub>1</sub>がホームネットワーク内のSAMであるか否かの検証も行う。

【0399】ステップS99-2: 前述したステップS99-4-2に対応する処理として、SAM305<sub>2</sub>は、SAM305<sub>1</sub>との間で相互認証を行って得たセ

セッション鍵データKSESを共有する。

ステップS99-3: SAM3052のSAM管理部190は、図94に示すように、ネットワーク機器3601のSAM3051からセキュアコンテナ304xを入力する。

ステップS99-4: 暗号化・復号部171は、ステップS99-2で共有したセッション鍵データKSESを用いて、SAM管理部190を介して入力したセキュアコンテナ304xを復号する。

【0400】ステップS99-5: セッション鍵データKSESを用いて復号されたセキュアコンテナ304x内のコンテンツファイルCFが、図94に示すメディア・ドライブSAM260におけるセクタライズ(Sectorize)・セクタヘッダの付加処理、スクランブル処理、ECCエンコード処理、変調処理および同期処理を経て、RAM型の記録媒体1304のRAM領域134に記録される。

【0401】ステップS99-6: セッション鍵データKSESを用いて復号されたセキュアコンテナ304x内の署名データSIG6, CP, SIG62, SP, SIG41, SAM1と、キーファイルKFおよびその署名データSIG7, CP, SIG63, SP, SIG42, SAM1と、キーファイルKF1およびそのハッシュ値HK1と、公開鍵署名データCERSpおよびその署名データSIG61, ESCと、公開鍵署名データCERCPおよびその署名データSIG1, ESCと、公開鍵署名データCERSAM1およびその署名データSIG22, ESCとが、作業用メモリ200に書き込まれる。

【0402】ステップS99-7: 署名処理部589において、作業用メモリ200から読み出された署名データSIG61, ESC, SIG1, ESC, SIG22, ESCが、記憶部192から読み出した公開鍵データKESC, Pを用いて検証され、公開鍵証明書データCERSp, CERCP, CERSAM1の正当性が確認される。そして、署名処理部589において、公開鍵証明書データCERCPに格納された公開鍵データKCP, Pを用いて、署名データSIG6, CPの正当性が検証され、コンテンツファイルCFの作成者の正当性が確認される。署名処理部589において、公開鍵証明書データCERSpに格納された公開鍵データKSP, Pを用いて、署名データSIG62, CPの正当性が検証され、コンテンツファイルCFの送信者の正当性が確認される。また、署名処理部189において、公開鍵証明書データCERSAM1に格納された公開鍵データKSAM1, Pを用いて、署名データSIG41, SAM1の正当性が検証され、コンテンツファイルCFの送信者の正当性が確認される。

【0403】ステップS99-8: 署名処理部589において、公開鍵証明書データCERCP, CERSp, CERSAM1に格納された公開鍵データKCP, P, KSP, KSAM1, Pを用いて、作業用メモリ200に記憶されている

署名データSIG7, CP, SIG63, SP, SIG42, SAM1の正当性を検証する。そして、署名データSIG7, CP, SIG63, SP, SIG42, SAM1が正当であると検証されたときに、キーファイルKFの送信者の正当性が確認される。

【0404】ステップS99-9: 署名処理部589において、記憶部192から読み出した公開鍵データKESC, Pを用いて、図97(B)のキーファイルKFに格納された署名データSIGK1, ESCの検証が行われる。そして、署名データSIGK1, ESCが正当であると検証されたときに、キーファイルKFの作成者の正当性が確認される。

【0405】ステップS99-10: 署名処理部189は、ハッシュ値HK1の正当性を検証し、キーファイルKF1の作成者および送信者の正当性を確認する。なお、当該例では、キーファイルKF1の作成者と送信元とが同じ場合を述べたが、キーファイルKF1の作成者と送信元とが異なる場合には、キーファイルKF1に対して作成者の署名データと送信者と署名データとが作成され、署名処理部189において、双方の署名データの正当性が検証される。

【0406】ステップS99-11: 利用監視部186は、ステップS99-10で復号されたキーファイルKF1に格納された利用制御データ166を用いて、以後のコンテンツデータの購入・利用形態を制御する。

【0407】ステップS99-12: ユーザは、購入・利用形態決定操作部165を操作して購入形態を決定し、当該操作に応じた操作信号S165が、課金処理部587に出力される。

ステップS99-13: 課金処理部587は、操作信号S165に基づいて、外部メモリ201に記憶されている利用履歴データ308を更新する。また、課金処理部587は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態に応じて利用制御データ166を更新する。

【0408】ステップS99-14: 暗号化・復号部173は、記憶部192から読み出した記録用鍵データKSTR・メディア鍵データKMEDおよび購入者鍵データKPINを順に用いて、ステップS99-12で生成された利用制御データ166を暗号化してメディア・ドライブSAM管理部855に出力する。

ステップS99-15: メディア・ドライブSAM管理部855は、新たな利用制御データ166を格納したキーファイルKF1を、セクタライズ処理、セクタヘッダの付加処理、スクランブル処理、ECCエンコード処理、変調処理および同期処理を経て、RAM型の記録媒体1304のセキュアRAM領域132に記録する。ステップS99-16: キーファイルKFが作業用メモリ200から読み出され、メディア・ドライブSAM管理部855を介して、図94に示すメディア・ドライブS

AM260によってRAM型の記録媒体130<sub>4</sub>のセキュアRAM領域132に書き込まれる。

【0409】ステップS99-17: CPU1100は、上述した処理が適切に行われたか否かを、外部割り込みでホストCPU810に通知する。なお、CPU1100は、上述した処理が適切に行われたか否かを示すSAMステータスレジスタのフラグを設定し、ホストCPU810がポーリングによって当該フラグを読んでもよい。

【0410】なお、SAM305<sub>1</sub>におけるROM型の記録媒体のコンテンツデータの購入形態決定処理、ROM型の記録媒体のコンテンツデータの購入形態を決定した後RAM型の記録媒体に書き込む場合の処理は、サービスプロバイダ310において秘密鍵データK<sub>SP</sub><sub>p</sub>を用いて付けられた署名データSIG<sub>SP</sub>の検証処理を行う点を除いて、前述した第1実施形態のSAM105<sub>1</sub>における処理と同じである。また、SAM305<sub>1</sub>の実現方法も、前述した第1実施形態で説明したSAM105<sub>1</sub>の実現方法と同じである。また、ユーザホームネットワーク303に用いられる機器においても、第1実施形態で説明した図63に示す構成は同様に適用される。また、この場合に、SAM305<sub>1</sub>、AV圧縮・伸長用SAM163、メディア・ドラブSAM260およびメディアSAM133の回路モジュールとして、図64～図79を用いて説明した構成が同様に適用される。また、図62を用いて説明したセキュア機能も、コンテンツプロバイダ101がサービスプロバイダ310に置き換える点を除いて、EMDシステム300でも同様に適用される。

【0411】以下、ユーザホームネットワーク303における各種の機器の接続形態等を再び説明する。図101は、ユーザホームネットワーク303における機器の接続形態の一例を説明するための図である。ここでは、図101に示すように、ユーザホームネットワーク303内でネットワーク機器360<sub>1</sub>、AV機器360<sub>2</sub>、360<sub>3</sub>がIEEE1394シリアルバス191を介して接続されている場合を説明する。ネットワーク機器360<sub>1</sub>は、外部メモリ201、SAM305<sub>1</sub>、CAモジュール311、AV圧縮・伸長用SAM163およびダウンロードメモリ167を有する。CAモジュール311は、公衆回線などのネットワークを介して、サービスプロバイダ310と通信を行う。また、SAM305<sub>1</sub>は、公衆回線などのネットワークを介して、EMDサービスセンタ302と通信を行う。ダウンロードメモリ167としては、メディアSAM167aを備えたメモリスティック、あるいはHDDなどが用いられる。ダウンロードメモリ167には、サービスプロバイダ310からダウンロードしたセキュアコンテンツ304などが記憶される。各機器には、ATRAC3やMPEGなどの各種の圧縮・伸長方式にそれぞれ対応した複数のAV圧

縮・伸長用SAM163が内蔵されている。SAM305<sub>1</sub>は、接触方式あるいは非接触方式のICカード1141と通信を行うことが可能である。ICカード1141は、ユーザIDなどの各種のデータが記憶しており、SAM305<sub>1</sub>においてユーザ認証を行う場合などに用いられる。

【0412】AV機器360<sub>2</sub>は、例えば、ストレージ機器であり、SAM305<sub>1</sub>と305<sub>2</sub>との間で所定の処理を経て、IEEE1394シリアルバス191を介してネットワーク機器360<sub>1</sub>から入力したセキュアコンテンツを記録媒体130に記録する。また、AV機器360<sub>3</sub>も同様に、例えば、ストレージ機器であり、SAM305<sub>2</sub>と305<sub>3</sub>との間で所定の処理を経て、IEEE1394シリアルバス191を介してAV機器360<sub>2</sub>から入力したセキュアコンテンツを記録媒体130に記録する。

【0413】なお、図101に示す例では、記録媒体130にメディアSAM133が搭載されている場合を例示したが、例えば、記録媒体130のメディアSAM133が搭載されていない場合には、図101に点線で示すように、メディア・ドラブSAM260を用いて、SAM305<sub>2</sub>、305<sub>3</sub>との間の認証が行われる。

【0414】次に、図82に示すEMDシステム300の全体動作について説明する。図102および図103は、EMDシステム300の全体動作のフローチャートである。ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテンツ304を送信する場合を例示して説明する。なお、以下に示す処理の前提として、EMDサービスセンタ302へのコンテンツプロバイダ301、サービスプロバイダ310およびSAM305<sub>1</sub>～305<sub>4</sub>の登録は既に終了しているものとする。

【0415】ステップS21: EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データK<sub>CP</sub><sub>p</sub>の公開鍵証明書CER<sub>CP</sub>を、自らの署名データSIG<sub>1</sub><sub>ESC</sub>と共にコンテンツプロバイダ301に送信する。また、EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データK<sub>SP</sub><sub>p</sub>の公開鍵証明書CER<sub>SP</sub>を、自らの署名データSIG<sub>61</sub><sub>ESC</sub>と共にサービスプロバイダ310に送信する。また、EMDサービスセンタ302は、各々有効期限が1カ月の3カ月のライセンス鍵データKD<sub>1</sub>～KD<sub>3</sub>をユーザホームネットワーク303のSAM305<sub>1</sub>～305<sub>4</sub>に送信する。

【0416】ステップS22: コンテンツプロバイダ301は、相互認証を行った後に、権利書データ106およびコンテンツ鍵データK<sub>c</sub>をEMDサービスセンタ302に登録して権威化する。また、EMDサービスセンタ302は、図3(B)に示す6カ月のキープファイルKFを作成し、これをコンテンツプロバイダ301に送

信する。

【0417】ステップS23：コンテンツプロバイダ301は、図3(A)、(B)に示すコンテンツファイルCFおよびその署名データSIG<sub>6</sub>、CPと、キーファイルKFおよびその署名データSIG<sub>7</sub>、CPとを作成し、これらと図3(C)に示す公開鍵証明書データCER<sub>CP</sub>およびその署名データSIG<sub>1</sub>、ESCとを格納したセキュアコンテナ104を、オンラインおよび/またはオフラインで、サービスプロバイダ310に提供する。

【0418】ステップS24：サービスプロバイダ310は、図3(C)に示す署名データSIG<sub>1</sub>、ESCを検証した後に、公開鍵証明書データCER<sub>CP</sub>に格納された公開鍵データK<sub>CP</sub>、Pを用いて、図3(A)、(B)に示す署名データSIG<sub>6</sub>、CPおよびSIG<sub>7</sub>、CPを検証して、セキュアコンテナ104が正当なコンテンツプロバイダ301から送信されたものであるかを確認する。

【0419】ステップS25：サービスプロバイダ310は、プライスタグデータ312およびその署名データSIG<sub>64</sub>、SPを作成し、これらを格納した格納した図87に示すセキュアコンテナ304を作成する。

【0420】ステップS26：サービスプロバイダ310は、プライスタグデータ312をEMDサービスセンタ302に登録して権威化する。

【0421】ステップS27：サービスプロバイダ310は、例えば、ユーザホームネットワーク303のCAモジュール311からの要求に応じて、ステップS25で作成したセキュアコンテナ304を、オンラインあるいはオフラインで、図89に示すネットワーク機器360<sub>1</sub>の復号モジュール905に送信する。

【0422】ステップS28：CAモジュール311は、SP用購入履歴データ309を作成し、これを所定のタイミングで、サービスプロバイダ310に送信する。

【0423】ステップS29：SAM305<sub>1</sub>～305<sub>4</sub>のいずれかにおいて、図84(D)に示す署名データSIG<sub>61</sub>、ESCを検証した後に、公開鍵証明書データCER<sub>SP</sub>に格納された公開鍵データK<sub>SP</sub>、Pを用いて、図84(A)、(B)、(C)に示す署名データSIG<sub>62</sub>、SP、SIG<sub>63</sub>、SP、SIG<sub>64</sub>、SPを検証して、セキュアコンテナ304内の所定のデータが正当なサービスプロバイダ310において作成および送信されたか否かを確認する。

【0424】ステップS30：SAM305<sub>1</sub>～305<sub>4</sub>のいずれかにおいて、図84(D)に示す署名データSIG<sub>1</sub>、ESCを検証した後に、公開鍵証明書データCER<sub>CP</sub>に格納された公開鍵データK<sub>CP</sub>、Pを用いて、図84(A)、(B)、(C)に示す署名データSIG<sub>6</sub>、SP、SIG<sub>7</sub>、SPを検証して、セキュアコンテナ304内のコンテンツファイルCFが正当なコンテンツプロバイダ301において作成されたか否かと、キーファイルKFが

正当なコンテンツプロバイダ301から送信されたか否かを確認する。また、SAM305<sub>1</sub>～305<sub>4</sub>のいずれかにおいて、公開鍵データK<sub>ESC</sub>、Pを用いて、図84(B)に示すキーファイルKF内の署名データSIG<sub>K1</sub>、ESCの正当性を検証することで、キーファイルKFが正当なEMDサービスセンタ302によって作成されたか否かを確認する。

【0425】ステップS31：ユーザが図88に示す操作部165を操作してコンテンツの購入・利用形態を決定する。

【0426】ステップS32：ステップS31においてホストCPU810からSAM305<sub>1</sub>～305<sub>4</sub>に出された内部割り込みS810に基づいて、SAM305<sub>1</sub>～305<sub>4</sub>において、セキュアコンテナ304の利用履歴(Usage Log)データ308が生成される。SAM305<sub>1</sub>～305<sub>4</sub>からEMDサービスセンタ302に、利用履歴データ308およびその署名データSIG<sub>205</sub>、SAM<sub>1</sub>が送信される。また、購入形態が決定される度にリアルタイムに、SAM305<sub>1</sub>～305<sub>4</sub>からEMDサービスセンタ302に利用制御状態データ166が送信される。

【0427】ステップS33：EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、決済請求権データ152c、152sを作成する。

【0428】ステップS34：EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c、152sを自らの署名データと共に送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310の所有者に分配される。

【0429】以上説明したように、EMDシステム300では、図3に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ301からサービスプロバイダ310に配給し、セキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFをそのまま格納したセキュアコンテナ304をサービスプロバイダ310からユーザホームネットワーク303に配給し、キーファイルKFについての処理をSAM305<sub>1</sub>～305<sub>4</sub>内で行う。また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD<sub>1</sub>～KD<sub>3</sub>を用いて暗号化されており、配信鍵データKD<sub>1</sub>～KD<sub>3</sub>を保持しているSAM305<sub>1</sub>～305<sub>4</sub>内での復号される。そして、SAM305<sub>1</sub>～305<sub>4</sub>では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデー

タCの購入形態および利用形態が決定される。

【0430】従って、EMDシステム300によれば、ユーザホームネットワーク303におけるコンテンツデータCの購入および利用を、サービスプロバイダ310における処理とは無関係に、コンテンツプロバイダ301の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。すなわち、EMDシステム300によれば、権利書データ106をサービスプロバイダ310が管理できないようである。そのため、EMDシステム300によれば、異系列の複数のサービスプロバイダ310を用いてユーザホームネットワーク303にコンテンツデータCが配給された場合でも、ユーザホームネットワーク303のSAMにおける当該コンテンツデータCについての権利処理を、コンテンツプロバイダ301が作成した共通の権利書データ106に基づいて行わせることができる。

【0431】また、EMDシステム300では、セキュアコンテナ104、304内の各ファイルおよびデータについて、それらの作成者および送信者の正当性を示す署名データを格納していることから、サービスプロバイダ310およびSAM305<sub>1</sub>～305<sub>4</sub>において、それらの作成者および送信者の正当性、並びにそれらが改竄されていないか否かなどを確認できる。その結果、コンテンツデータCの不正利用を効果的に回避できる。

【0432】また、EMDシステム300では、サービスプロバイダ310からユーザホームネットワーク303へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ304を用いて行うことで、双方の場合において、SAM305<sub>1</sub>～305<sub>4</sub>におけるコンテンツデータCの権利処理を共通化できる。

【0433】また、EMDシステム300では、ユーザホームネットワーク303内のネットワーク機器360<sub>1</sub>およびAV機器360<sub>2</sub>～360<sub>4</sub>においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。例えば、図104に示すように、コンテンツプロバイダ301が提供したコンテンツデータCを、サービスプロバイダ310からユーザホームネットワーク303に、パッケージ流通、デジタル放送、インターネット、専用線、デジタルラジオおよびモバイル通信などの何れの手法（経路）で配信（配給）した場合でも、ユーザホームネットワーク303、303aのSAMにおいて、コンテンツプロバイダ301が作成した権利書データ106に基づいて、共通の権利処理ルールが採用される。

【0434】また、EMDシステム300によれば、EMDサービスセンタ302が、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額

が、コンテンツプロバイダ301およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。また、EMDシステム300によれば、同じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービスプロバイダ310のサービス形態とは無関係に、そのままSAM305<sub>1</sub>～305<sub>4</sub>に供給される。従って、SAM305<sub>1</sub>～305<sub>4</sub>において、権利書データ106に基づいて、コンテンツプロバイダ301の意向通りに、コンテンツファイルCFの利用を行わせることができる。すなわち、EMDシステム300によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織725に頼ることなく、技術的な手段によって、コンテンツプロバイダ301の所有者の権利および利益を確実に守ることができる。

【0435】以下、上述した第2実施形態のEMDシステム300で採用するセキュアコンテナなどの配信プロトコルについて説明する。図105に示すように、コンテンツプロバイダ301において作成されたセキュアコンテナ104は、インターネット（TCP/IP）あるいは専用線（ATM Cell）などのコンテンツプロバイダ用配信プロトコルを用いてサービスプロバイダ310に提供される。また、サービスプロバイダ310は、セキュアコンテナ104を用いて作成したセキュアコンテナ304を、デジタル放送（MPEG-TS上のXML/SMIL）、インターネット（TCP/IP上のXML/SMIL）あるいはパッケージ流通（記録媒体）などのサービスプロバイダ用配信プロトコルを用いてユーザホームネットワーク303に配給する。また、ユーザホームネットワーク303、303a内、あるいはユーザホームネットワーク303と303aとの間において、SMA相互間で、セキュアコンテナが、家庭内EC（Electric Commerce）/配信サービス（1394シリアルバス・インターフェイス上のXML/SMIL）や記録媒体などを用いて転送される。

【0436】本発明は上述した実施形態には限定されない。例えば、上述した実施形態では、EMDサービスセンタ102、302において、キーファイルKFを作成する場合を示したが、コンテンツプロバイダ101、301においてキーファイルKFを作成してもよい。

【0437】

【発明の効果】以上説明したように、本発明のデータ処理装置によれば、コンテンツデータの取り扱いを示す権利書データに基づいたコンテンツデータの権利処理をセキュアな環境で行うことができる。その結果、権利書データをコンテンツデータの提供に係わる者が作成すれば、コンテンツデータに係わる利益を適切に保護することが可能になると共に、当該関係者による監査の負担を軽減できる。



【図面の簡単な説明】

【図1】図1は、本発明の第1実施形態のEMDシステムの全体構成図である。

【図2】図2は、本発明のセキュアコンテナの概念を説明するための図である。

【図3】図3は、図1に示すコンテンツプロバイダからSAMに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図4】図4は、図3に示すコンテンツファイルに含まれるデータを詳細に説明するための図である。

【図5】図5は、図3に示すキーファイルに含まれるデータを詳細に説明するための図である。

【図6】図6は、図1に示すコンテンツプロバイダとEMDサービスセンタとの間で行われる登録およびキーファイルの転送を説明するための図である。

【図7】図7は、コンテンツファイルに格納されるヘッダデータを説明するための図である。

【図8】図8は、コンテンツIDを説明するための図である。

【図9】図9は、セキュアコンテナのディレクトリ構造を説明するための図である。

【図10】図10は、セキュアコンテナのハイパーリンク構造を説明するための図である。

【図11】図11は、本実施形態で用いられるROM型の記録媒体の第1の例を説明するための図である。

【図12】図12は、本実施形態で用いられるROM型の記録媒体の第2の例を説明するための図である。

【図13】図13は、本実施形態で用いられるROM型の記録媒体の第3の例を説明するための図である。

【図14】図14は、本実施形態で用いられるRAM型の記録媒体の第1の例を説明するための図である。

【図15】図15は、本実施形態で用いられるRAM型の記録媒体の第2の例を説明するための図である。

【図16】図16は、本実施形態で用いられるRAM型の記録媒体の第3の例を説明するための図である。

【図17】図17は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図18】図18は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図19】図19は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図20】図20は、図1に示すEMDサービスセンタの機能を説明するための図である。

【図21】図21は、図1に示す利用履歴データを説明するための図である。

【図22】図22は、図1に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図23】図23は、図2に示すホストCPUとSAMとの関係を説明するための図である。

【図24】図24は、SAMを実現するソフトウェア構成を説明するための図である。

【図25】図25は、ホストCPUに出される外部割り込みを説明するための図である。

【図26】図26は、ホストCPUが出す内部割り込みを説明するための図である。

【図27】図27は、ホストCPUが出すファンクションコールを説明するための図である。

【図28】図28は、SAMのCPOUの処理状態を説明するための図である。

【図29】図29は、ホストCPUおよびSAMのメモリ空間を説明するための図である。

【図30】図30は、図1に示すユーザホームネットワーク内のSAMの機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでのデータの流れを示す図である。

【図31】図31は、図2に示す外部メモリに記憶されるデータを説明するための図である。

【図32】図32は、作業用メモリに記憶されるデータを説明するための図である。

【図33】図33は、図1に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図34】図34は、図30に示す記憶部に記憶されるデータを説明するための図である。

【図35】図35は、EMDサービスセンタからライセンス鍵データを受信する際のSAMの処理を示すフローチャートである。

【図36】図36は、セキュアコンテナを入力する際のSAMの処理を示すフローチャートである。

【図37】図37は、図1に示すユーザホームネットワーク内のSAMの機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図38】図38は、コンテンツデータの購入形態を決定する際のSAMの処理を示すフローチャートである。

【図39】図39は、購入形態が決定されたセキュアコンテナを説明するための図である。

【図40】図40は、コンテンツデータを再生する際のSAMの処理を示すフローチャートである。

【図41】図41は、図2に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV機器のSAMに転送し、AV機器において再購入を行う場合を説明するための図である。

【図42】図42は、図41に示す場合における転送元のSAM内でのデータの流れを示す図である。

【図43】図43は、図42に示す場合の処理を示すフローチャートである。

【図44】図44は、図41において転送されるセキュアコンテナのフォーマットを説明するための図である。

【図45】図45は、図41に示す場合において、転送先のSAMにおいて、入力したコンテンツファイルなどを、RAM型あるいはROM型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図46】図46は、図41に示す場合における転送先のSAMの処理を示すフローチャートである。

【図47】図47は、図41に示す場合における転送先のSAMの処理を示すフローチャートである。

【図48】図48は、図1に示すユーザホームネットワーク内のSAMにおける各種の購入形態を説明するための図である。

【図49】図49は、コンテンツの購入形態が未決定の図11に示すROM型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV機器において購入形態を決定する場合を説明するための図である。

【図50】図50は、図49に示す場合におけるAV機器のSAM内でのデータの流れを示す図である。

【図51】図51は、図49に示す場合におけるSAMの処理のフローチャートである。

【図52】図52は、ユーザホームネットワーク内のAV機器において購入形態が未決定のROM型の記録媒体からセキュアコンテナを読み出して、これを他のAV機器に転送してRAM型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図53】図53は、図52に示す場合における転送元のSAM内でのデータの流れを示す図である。

【図54】図54は、図52において、転送元のSAMから転送先のSAMに転送されるセキュアコンテナのフォーマットを説明するための図である。

【図55】図55は、図52の場合における、転送元および転送先のSAMの処理のフローチャートを示す図である。

【図56】図56は、図52の場合における、転送元および転送先のSAMの処理のフローチャートを示す図である。

【図57】図57は、図52に示す場合における転送先のSAM内でのデータの流れを示す図である。

【図58】図58は、ユーザホームネットワーク内でのバスへの機器の接続形態の一例を説明するための図である。

【図59】図59は、SAMが作成するSAM登録リストのデータフォーマットを説明するための図である。

【図60】図60は、EMDサービスセンタが作成する公開鍵証明書破棄リストのフォーマットを説明するための図である。

【図61】図61は、EMDサービスセンタが作成するSAM登録リストのデータフォーマットを説明するため

の図である。

【図62】図62は、SAMが持つセキュリティ機能を説明するための図である。

【図63】図62は、図1に示すユーザホームネットワーク内の例えばネットワーク機器内での各種のSAMに搭載形態の一例を説明するための図である。

【図64】図64は、図63に示すダウンロードメモリ周辺の詳細な回路構成を説明するための図である。

【図65】図65は、図63におけるホストCPUとSAMとの関係を説明するための図である。

【図66】図66は、図63におけるホストCPU、SAM、AV圧縮・伸長用SAMおよび記録媒体の関係を説明するための図である。

【図67】図67は、図63におけるホストCPU、メディア・ドラブSAMおよびAV圧縮・伸長用SAMの関係を説明するための図である。

【図68】図68は、権利処理用のSAMの回路モジュールの第1形態を説明するための図である。

【図69】図69は、図68に示す回路モジュールを用いた場合のSAM内のハードウェア構成の一例を説明するための図である。

【図70】図70は、権利処理用のSAMのアドレス空間を説明するための図である。

【図71】図71は、ホストCPUのアドレス空間を説明するための図である。

【図72】図72は、権利処理用のSAMの回路モジュールの第2形態を説明するための図である。

【図73】図73は、メディアSAMの回路モジュールを説明するための図である。

【図74】図74は、ROM型の記録媒体のメディアSAMの出荷時における記憶データを説明するための図である。

【図75】図75は、ROM型の記録媒体のメディアSAMの登録後における記憶データを説明するための図である。

【図76】図76は、RAM型の記録媒体のメディアSAMの出荷時における記憶データを説明するための図である。

【図77】図77は、RAM型の記録媒体のメディアSAMの登録後における記憶データを説明するための図である。

【図78】図78は、AV圧縮・伸長用SAMの回路モジュールの第1形態を説明するための図である。

【図79】図79は、メディア・ドラブSAMの回路モジュールを説明するための図である。

【図80】図80は、図1に示すEMDシステムの全体動作のフローチャートである。

【図81】図81は、第1実施形態のEMDシステムにおいて用いられるセキュアコンテナの配送プロトコルの一例を説明するための図である。

【図82】図82は、本発明の第2実施形態のEMDシステムの全体構成図である。

【図83】図83は、サービスプロバイダにおいて行われるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図84】図84は、図82に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図85】図85は、図84に示すセキュアコンテナに格納されたコンテンツファイルの送信形態を説明するための図である。

【図86】図86は、図87に示すセキュアコンテナに格納されたキーファイルの送信形態を説明するための図である。

【図87】図87は、図81に示すEMDサービスセンタの機能を示す図である。

【図88】図88は、図82に示すネットワーク機器の構成図である。

【図89】図89は、図88に示すCAモジュールの機能ブロック図である。

【図90】図90は、図82に示すSAMの機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図91】図91は、図90に示す作業用メモリに記憶されるデータを説明するための図である。

【図92】図92は、図82に示すSAMの機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図93】図93は、図82に示すSAMにおけるセキュアコンテナの入力処理の手順を示すフローチャートである。

【図94】図94は、図82に示すネットワーク機器のダウンロードメモリにダウンロードされた既に入力形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合を説明するための図である。

【図95】図95は、図82に示すネットワーク機器のダウンロードメモリにダウンロードされた既に入力形態が決定されたコンテンツファイルを、AV機器のSAMに転送する場合の転送元のSAM内での処理の流れを説明するための図である。

【図96】図96は、図95に示す転送元のSAMの処理を示すフローチャートである。

【図97】図97は、図94に示す場合に、転送元のSAMから転送先のSAMに転送されるセキュアコンテナのフォーマットを示す図である。

【図98】図98は、図94に示す場合の転送先のSAM内でのデータの流れを示す図である。

【図99】図99は、図94に示す場合の転送先のSAMの処理のフローチャートである。

【図100】図100は、図94に示す場合の転送先のSAMの処理のフローチャートである。

【図101】図101は、図82に示すユーザホームネットワーク内でのSAMの接続形態の一例を説明するための図である。

【図102】図102は、図82に示すEMDシステムの全体動作のフローチャートである。

【図103】図103は、図82に示すEMDシステムの全体動作のフローチャートである。

【図104】図104は、図82に示すEMDシステムのサービス形態の一例を示す図である。

【図105】図105は、図82に示すEMDシステムにおいて採用されるセキュアコンテナの配送プロトコルを説明するための図である。

【図106】図106は、従来のEMDシステムの構成図である。

#### 【符号の説明】

90…ペイメントゲートウェイ、91…決済機関、92…ルート認証局、100、300…EMDシステム、101、301…コンテンツプロバイダ、102、302…EMDサービスセンタ、103、303…ユーザホームネットワーク、104、304…セキュアコンテナ、105<sub>1</sub>～105<sub>4</sub>、305<sub>1</sub>～305<sub>4</sub>…SAM、106…権利書データ、107、307…決済レポートデータ、108、308…利用履歴データ、160<sub>1</sub>…ネットワーク機器、160<sub>2</sub>～160<sub>4</sub>…AV機器、152、152c、152s…決済請求権データ、191…バス、310…サービスプロバイダ、311…CAモジュール、312…プライスタグデータ、CF…コンテンツファイル、KF…キーファイル、Kc…コンテンツ鍵データ

【図31】

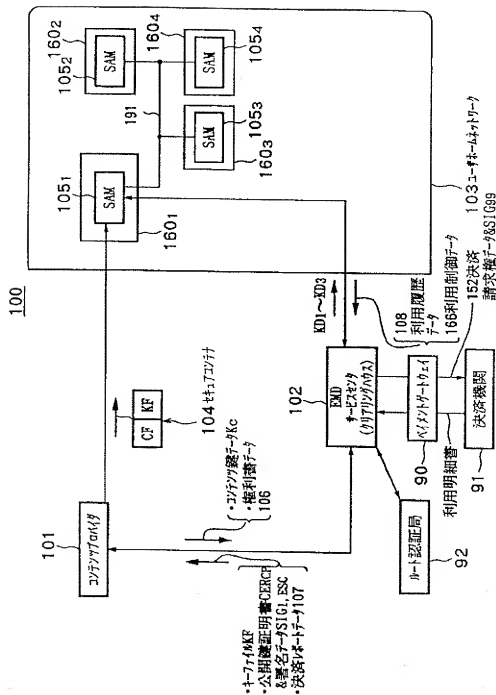
#### 外部メモリ201に記憶されるデータ

利用履歴データ108

SAM登録料

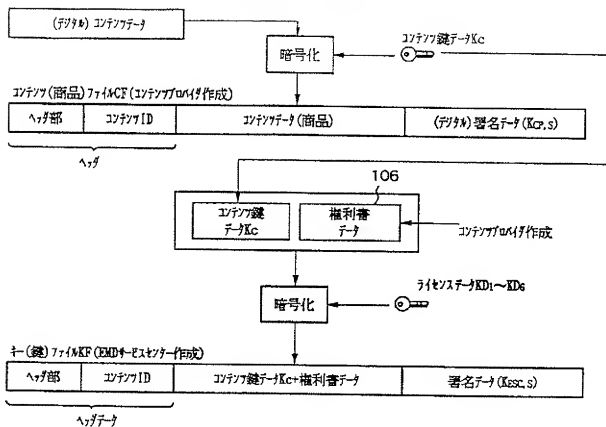
(KFがダウンロードメモリがないSAMが無い場合)

【図1】

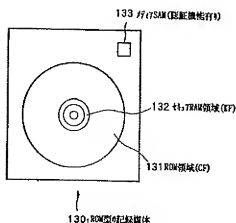


【図2】

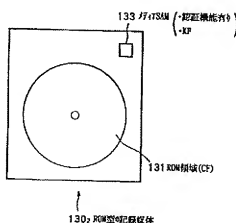
本発明のコンテンツの概念



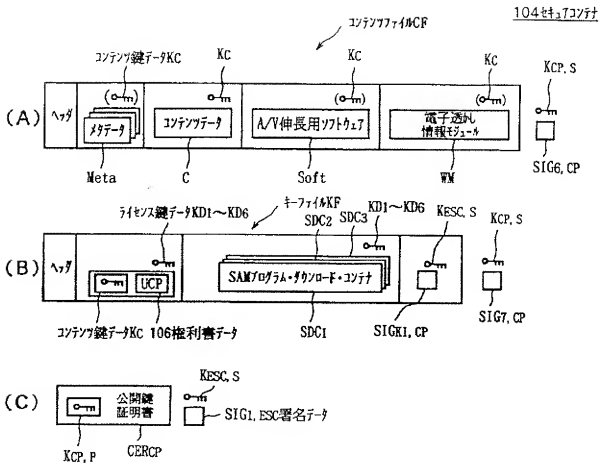
【図11】



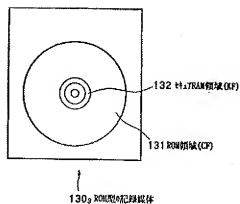
【図12】



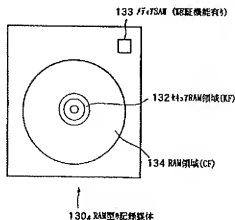
【図3】



【図13】

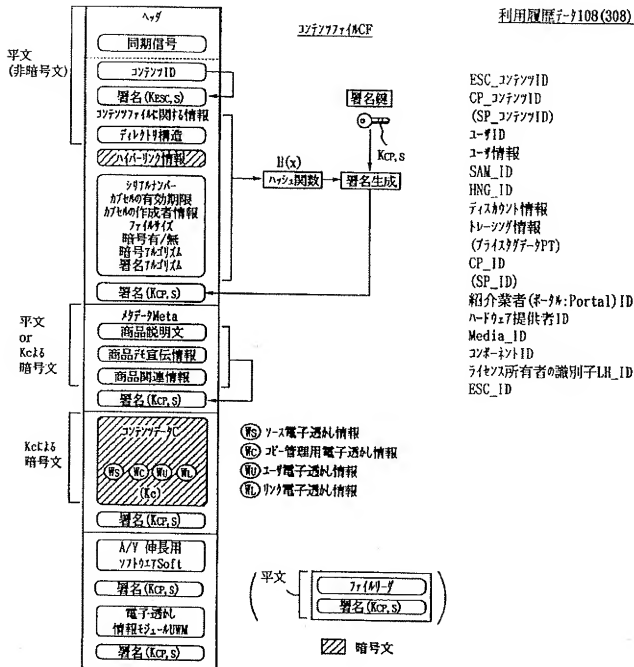


【図14】



【図4】

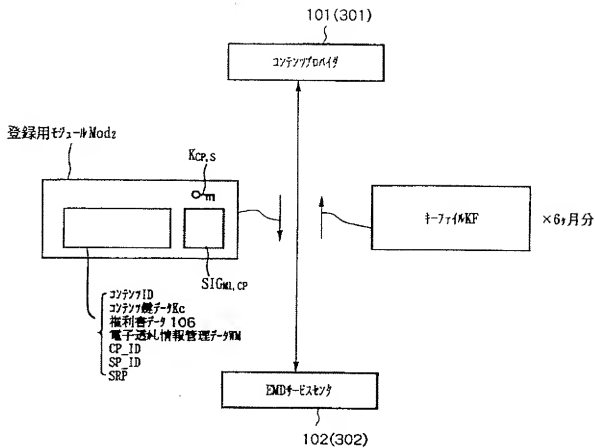
【図21】



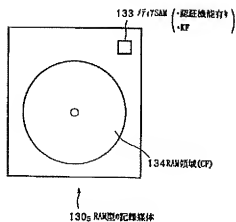




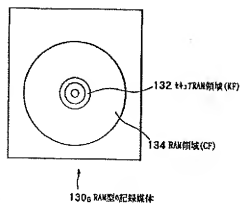
【図6】



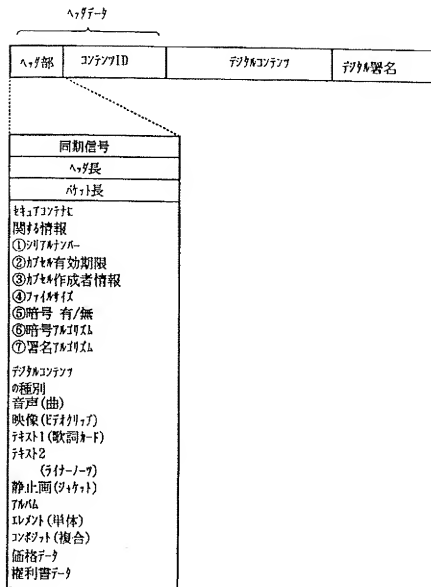
【図15】



【図16】



【図 7】

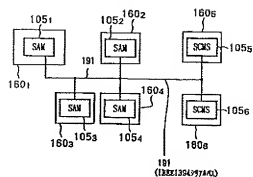


【図 3 2】

作業用メモリ200に記憶されるデータ

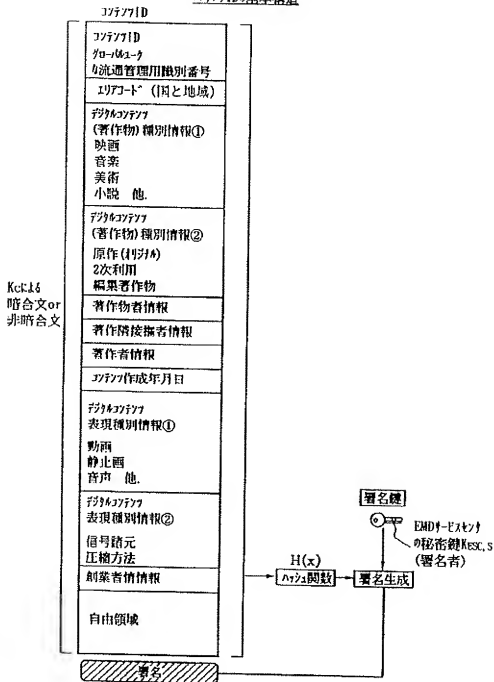
コンテンツ鍵データKc  
 権利書データ(UCP) 106  
 記憶部(フラッシュメモリ) 192のロック鍵データKLoc  
 コンテンツプロバイダ101の公開鍵証明書CERcp  
 利用制御データ(UCS) 166  
 SAMプログラム・ダウンロード・コンテンツSD1～SDC3

【図 5 8】

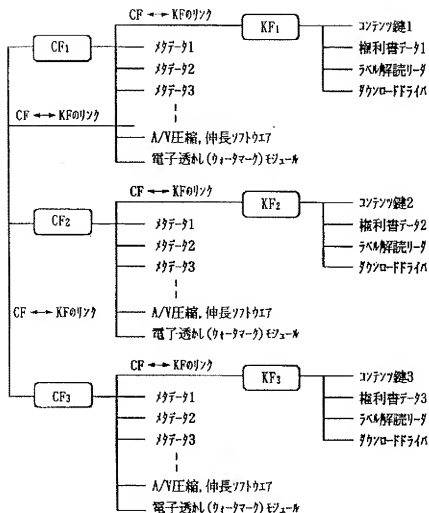


【図8】

## デジタルIDの基本構造



【図9】

セキュアコンテナのディレトリ構造

【図9 1】

作業用メモリ200の記憶データ

コンテンツ鍵データKc

権利書データ(UCP)106

不揮発性メモリ201のロック鍵データK<sub>LOC</sub>コンテンツプロバイダ301の公開鍵証明書データCER<sub>CP</sub>サービスプロバイダ301の公開鍵証明書データCER<sub>SP</sub>

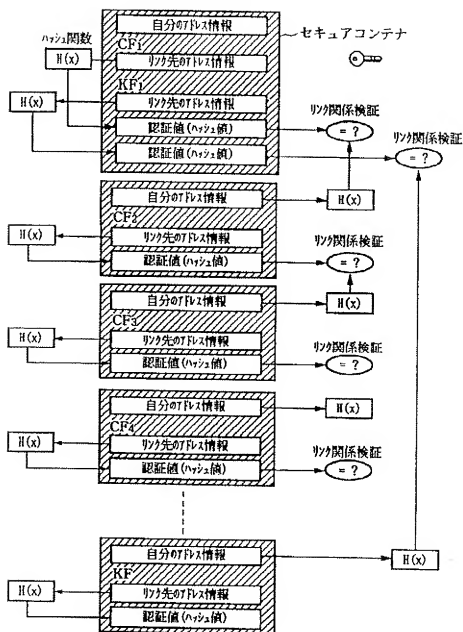
利用制御データ(UCS)166

SAMプログラム・ダウンロード・コンテナSD<sub>1</sub>~SD<sub>3</sub>

プレイスリダデータ312

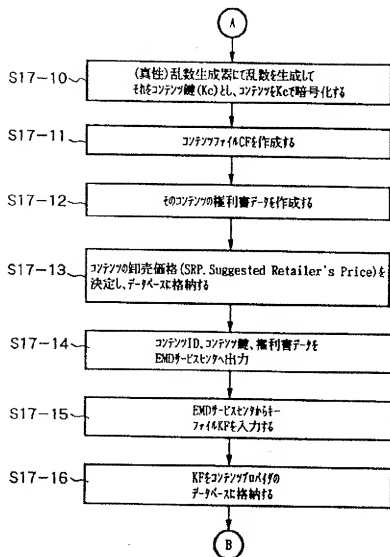
【図10】

セキュリティコンテナのハッシュ関数

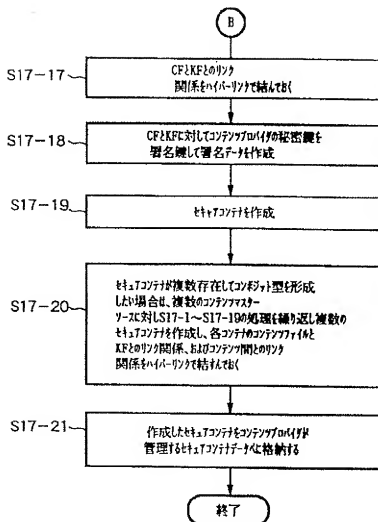




【図18】



【図19】





【図20】

## EMDサービス102の主な機能

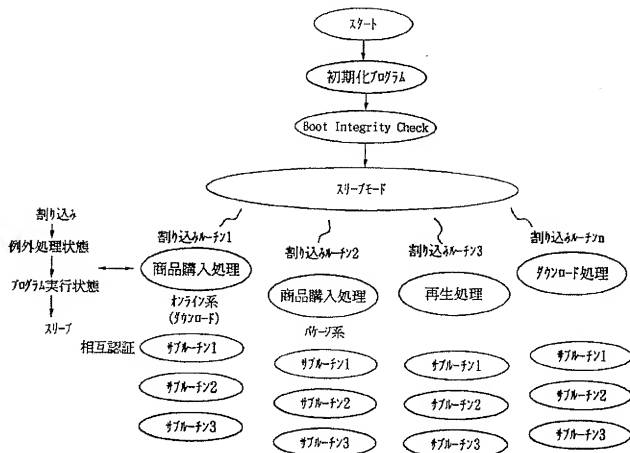
ライセンス鍵データをコンテンツプロバイダおよびSAMに供給

公開鍵証明書データCERcp, CERsamt~CERsamの発行

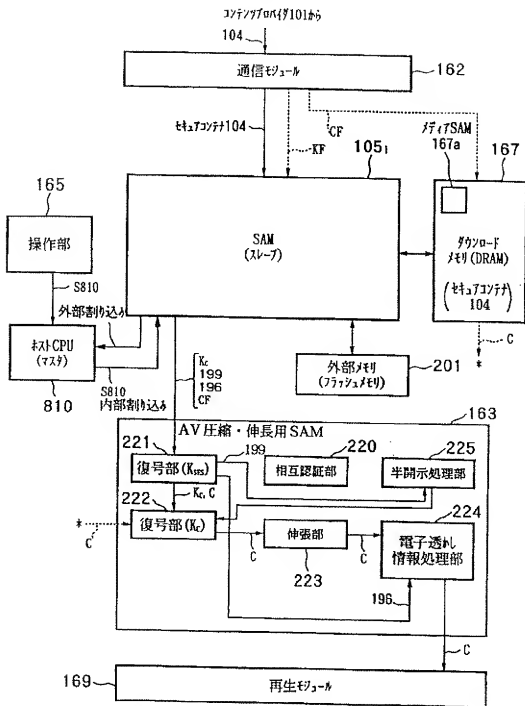
キーファイルKFの生成

利用履歴データに基づいた決済処理(利益分配処理)

【図24】



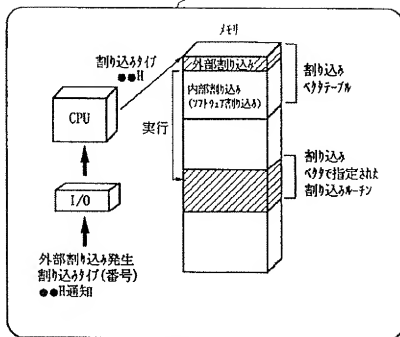
【図22】





【図 25】

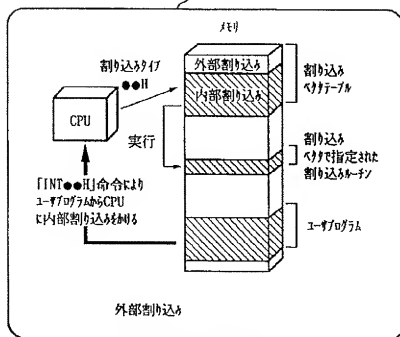
810 主CPU



ハードウェア割り込み (外部割り込み)

【図 26】

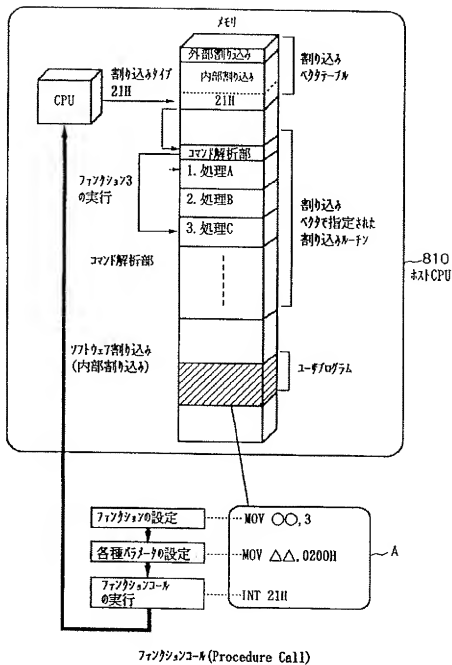
810 主CPU



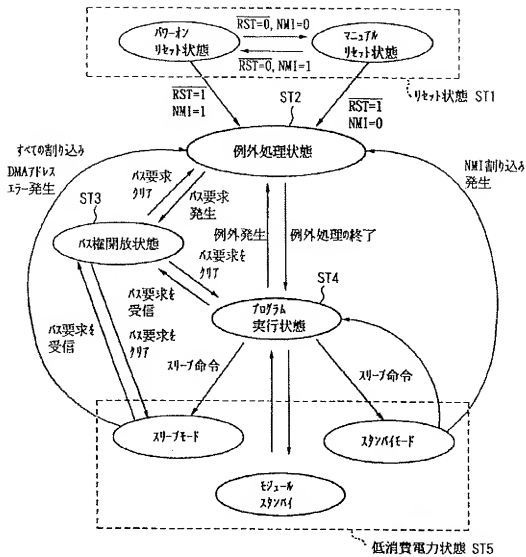
外部割り込み

ソフトウェア割り込み (内部割り込み)

【図27】



【図28】



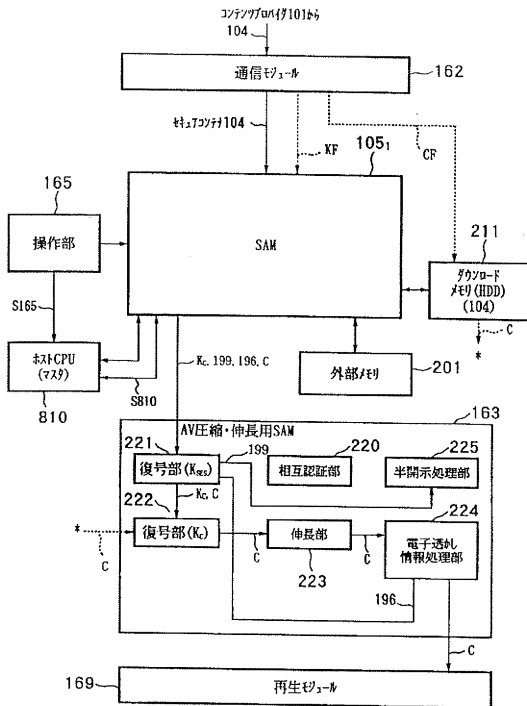
SAM0CPUの処理状態





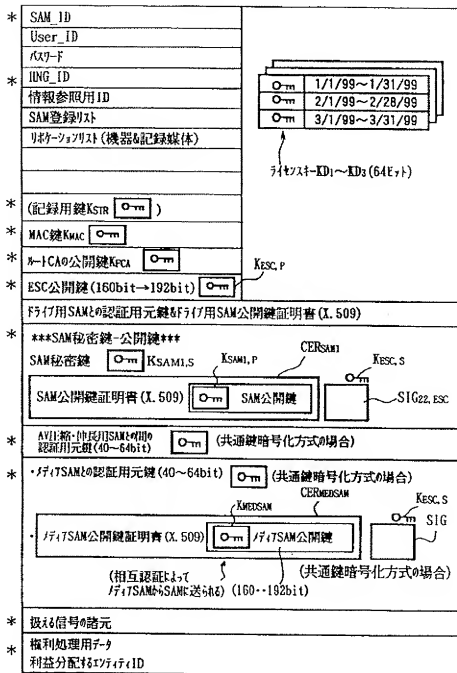


【図33】

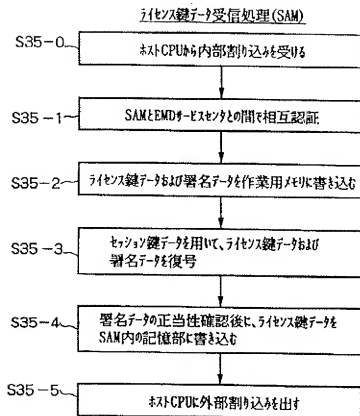


【図34】

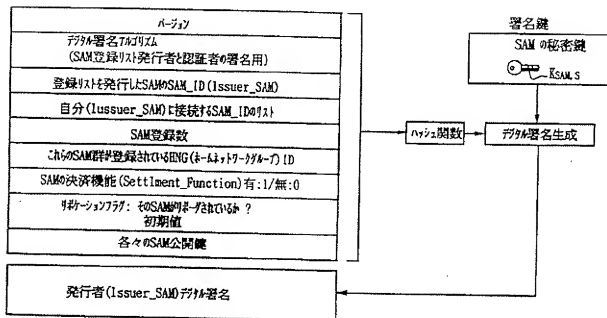
## 記憶部192に記憶されるデータ



【図35】

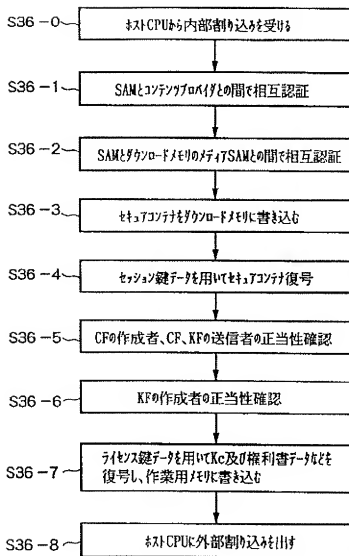


【図59】

SAM登録リスト (SAM Registration List) (SAM#作成)

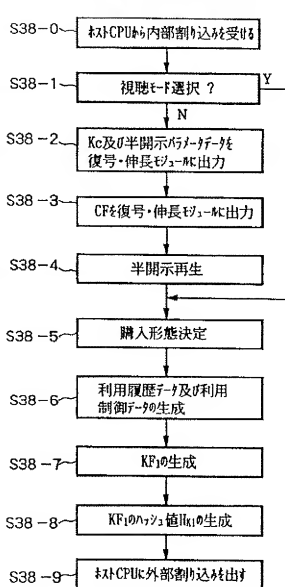
【図36】

## セキアコンテナの入力処理(SAW)

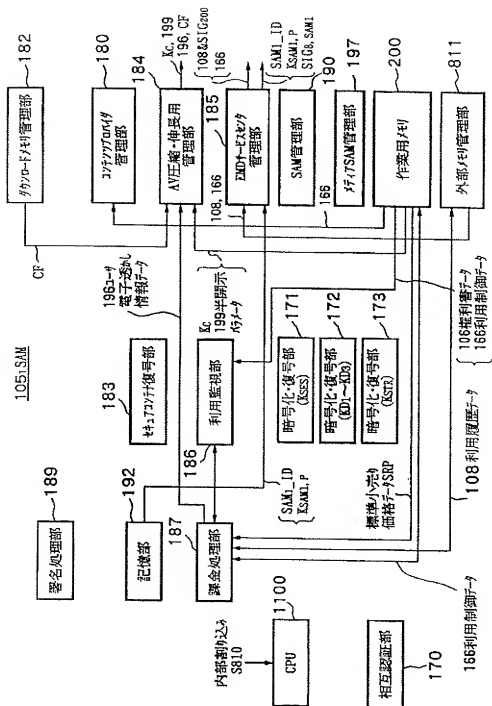


【図38】

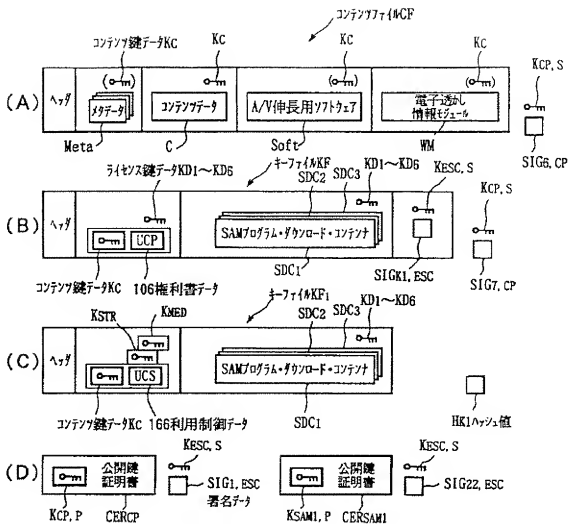
## 購入形態決定処理(SAW)



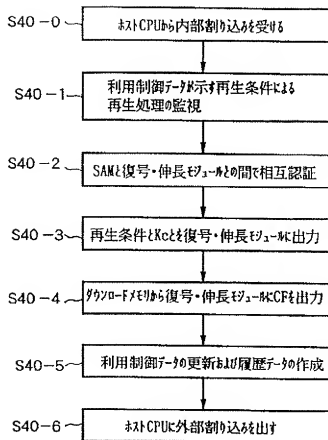
【圖 3 7】



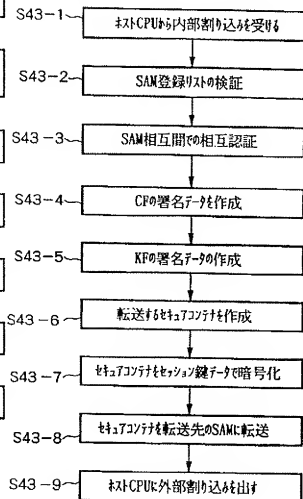
【図39】



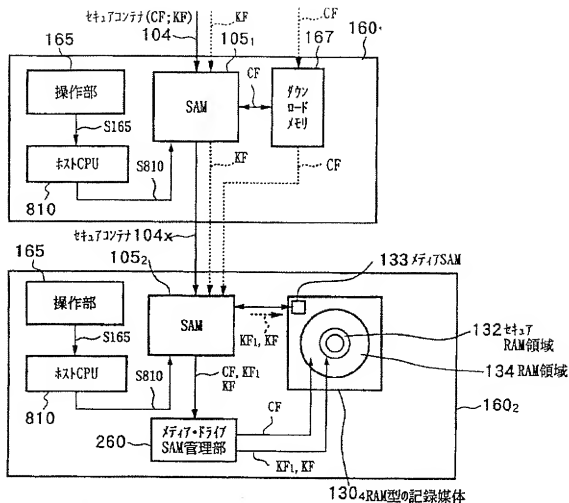
【図40】

コンテナデータの再生処理 (SAM)

【図43】

一の機器の利用制御データを使用して他の機器で再購入を行う場合の転送元のSAMの処理

【図41】





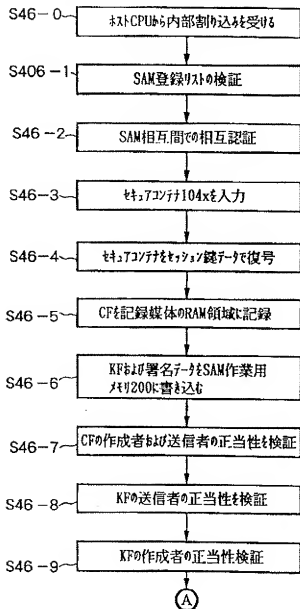




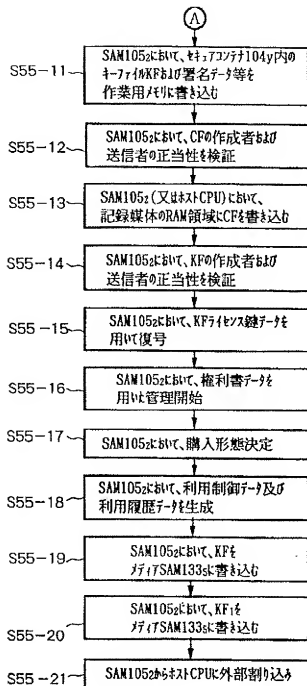


【図46】

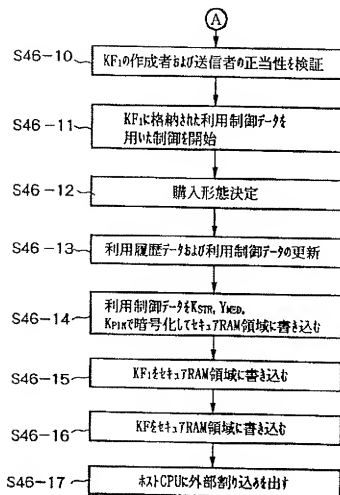
一の機器の利用制御データを使用して他の機器で  
再購入を行う場合の転送先のSAMの処理



【図56】

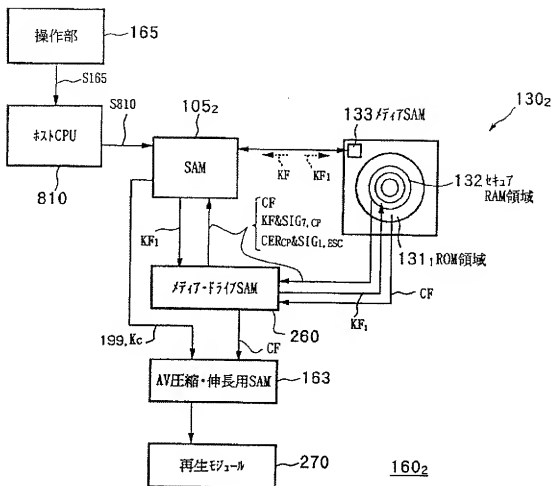


【図47】





【図49】

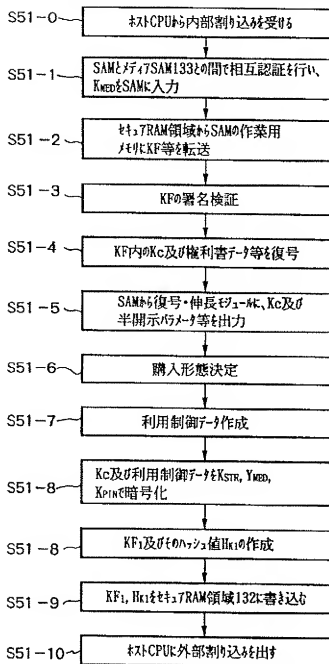




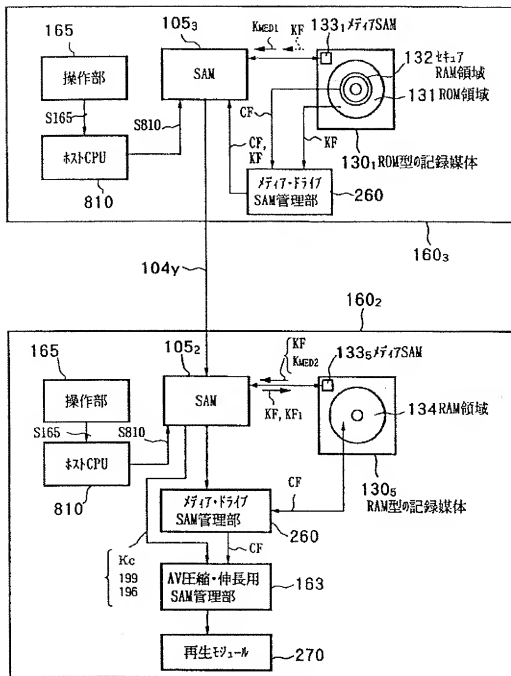


【図51】

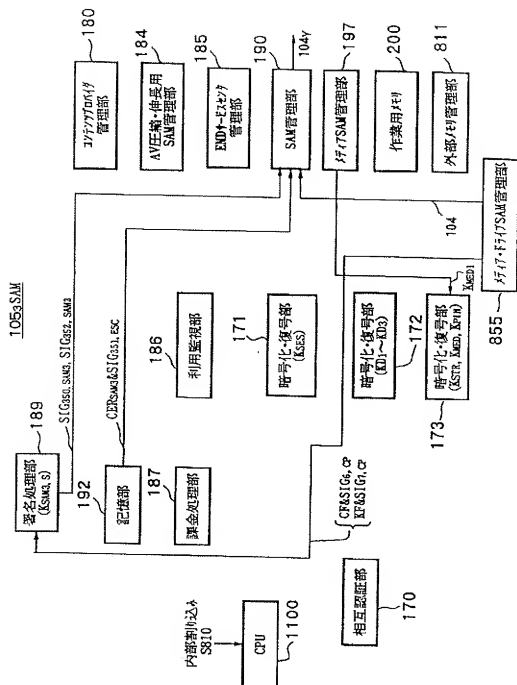
## ROM型の記録媒体のコンテナデータの購入形態決定処理



【図52】



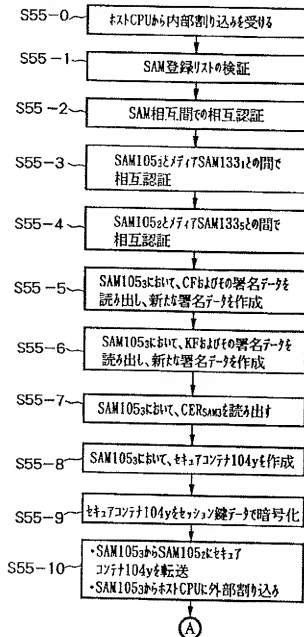
[図53]





【図55】

ROM型の記録媒体のコンテナデータを転送した後転送先で  
購入形態を決定してRAM型の記録媒体に書き込む場合の処理

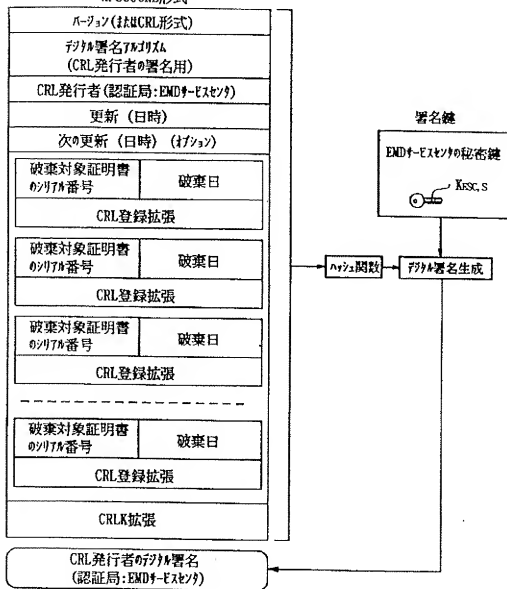




【図60】

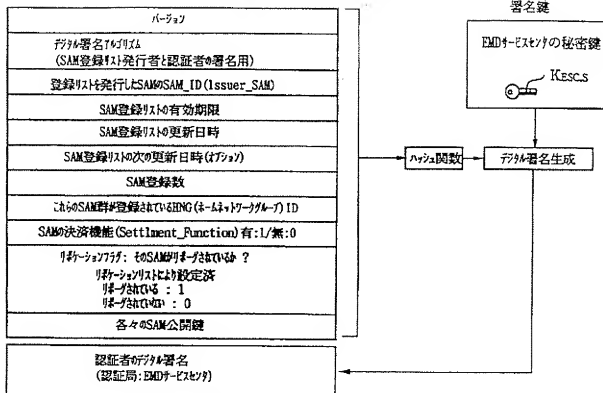
## 公開鍵証明書破棄リスト (CRL: Certificate Revocation List)

## X.509CRL形式

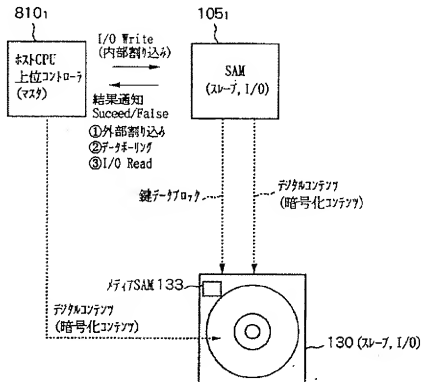


【図61】

## SAM登録リスト (EMDサービスセンサ作成)

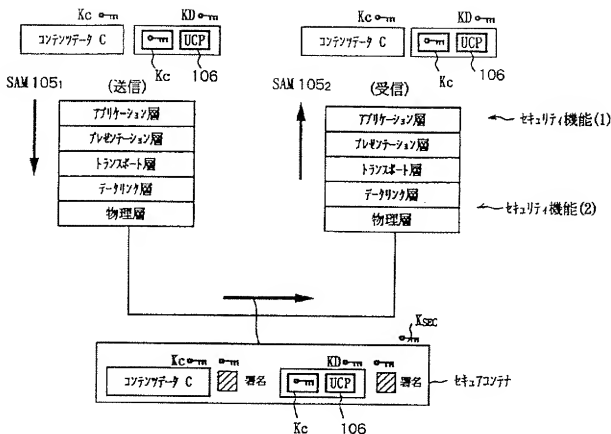


【図65】

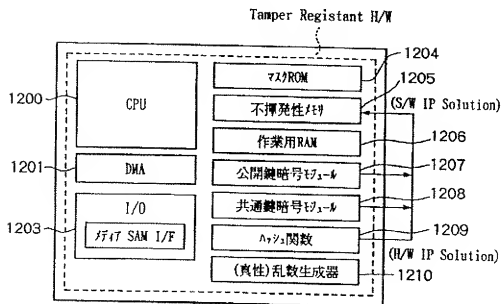




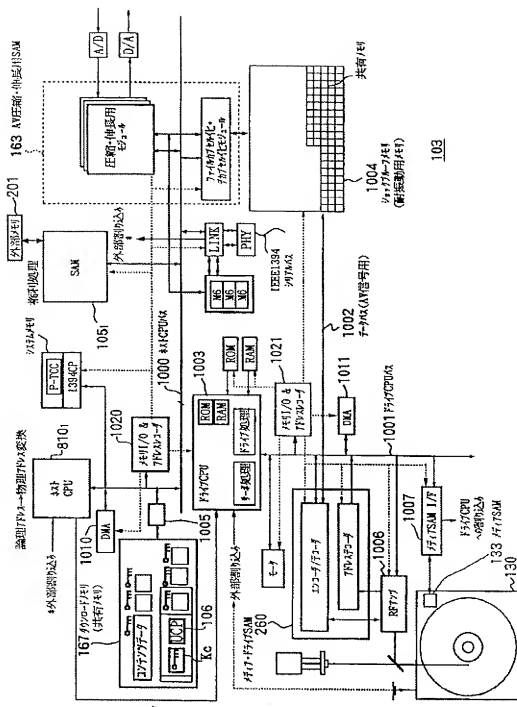
【図62】



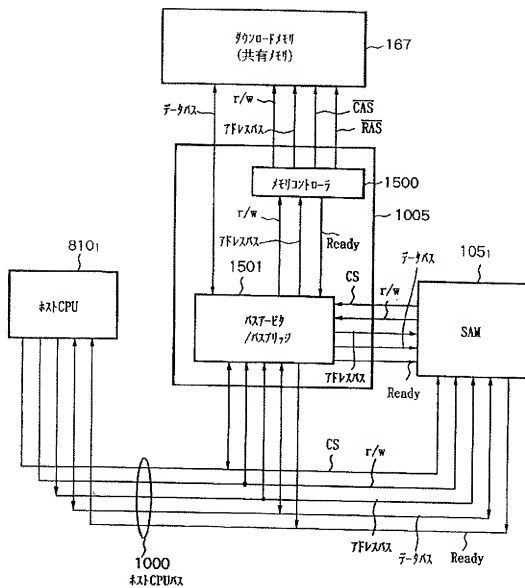
【図73】



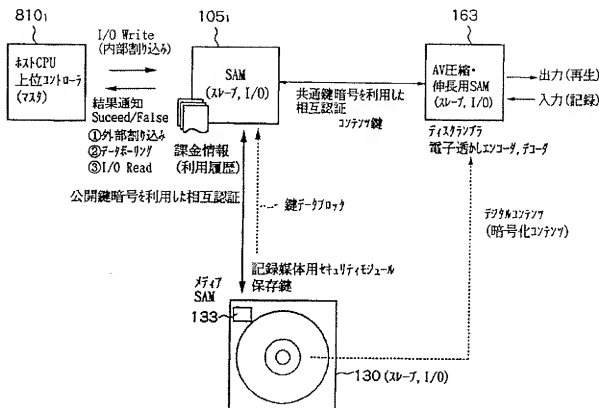
[図63]



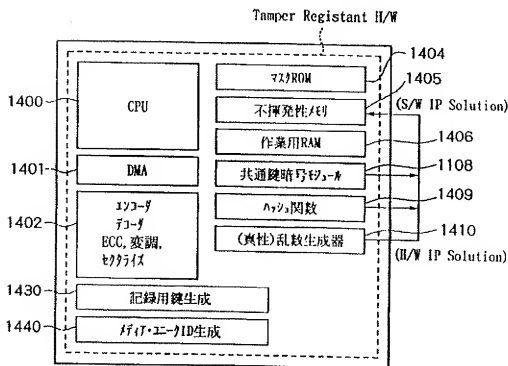
【図64】



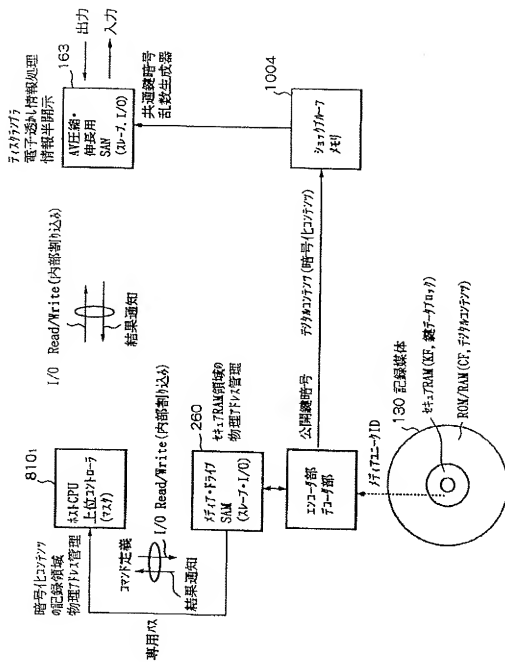
【図66】



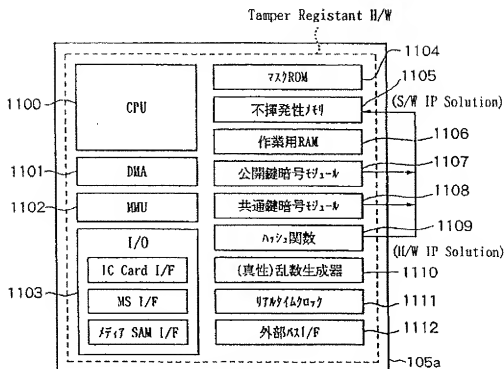
【図79】



【図67】



【図68】



権利処理用のSAM105a

【図87】

EMDサービス302の主な機能

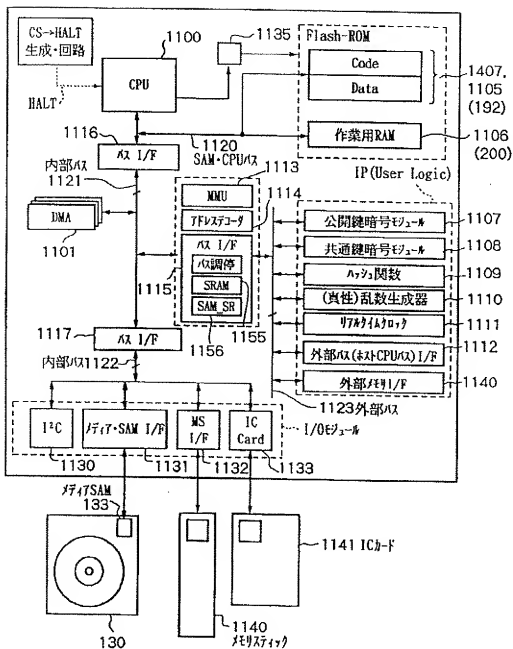
ライセンス鍵データをコンテンツプロバイダおよびSAMに供給

公開鍵証明書データDERCP, CERSP, CERSAM1～CERSAM4の発行

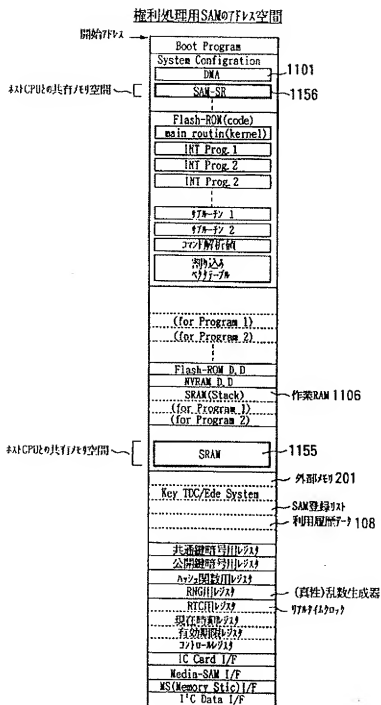
キーファイルKFの生成

利用履歴データに基づいた決済処理  
(CPとSPとの間の利益分配処理)

【圖 69】



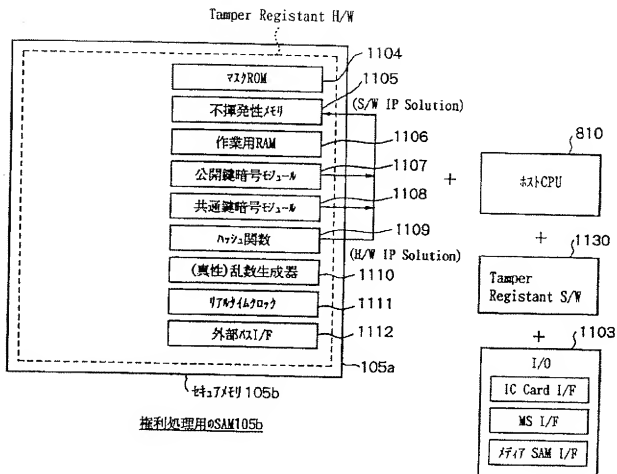
【図70】







【図72】



【図74】

ディTSAM ID	
記録用鍵KSTR(ディ鍵KMD)	
第3信頼機関(EMDサービス)の公開鍵	
ルートCAの公開鍵	
ディTSAM公開鍵証明書(X.509)	
ディTSAM公開鍵・秘密鍵	
Revocation List(更新値)	
権利処理(利益配分)用データ	
利益分配と関連エンティティのID	
ディタイプ	
・ディ70種別情報	
・ROM/RAM	
キーファイルKFの物理アドレス情報 (レジスタ空間)	検証値
検証値(MAC)	
コンテンツナンバー-#10KF	
コンテンツナンバー-#20KF	
コンテンツナンバー-#30KF	
コンテンツナンバー-#40KF	
コンテンツナンバー-#50KF	
	検証値(MAC)
コンテンツナンバー-#n0KF	
検証値(MAC)	

ライセンス鍵KDKによる  
暗号文

ROM型の記録媒体のディTSAMの記憶データ(出荷時)

【図75】

ディTSAM ID	
記録用鍵KSTR(ディ鍵KMD)	
User ID	
パスワード	
個人嗜好情報	
個人決済情報(クレジットカード番号)	
電子マネー	
第3信頼機関(EMDサービス)の公開鍵	
ルートCAの公開鍵	
ディTSAM公開鍵証明書(X.509)	
ディTSAM公開鍵・秘密鍵	
Revocation List(更新値)	
権利処理(利益配分)用データ	
利益分配に関関連エンティティのID	
ディタイプ	
・ディの種別情報	
・ROM/RAM	
キーファイルKFの物理アドレス情報 (レジスタ空間)	検証値
検証値(MAC)	
コンテンツ番号-#1のKF/KF <sub>1</sub>	
コンテンツ番号-#2のKF/KF <sub>1</sub>	
コンテンツ番号-#3のKF/KF <sub>1</sub>	
コンテンツ番号-#4のKF/KF <sub>1</sub>	
コンテンツ番号-#5のKF/KF <sub>1</sub>	
	検証値 (MAC)
コンテンツ番号-#nのKF/KF <sub>1</sub>	
検証値(MAC)	

ライセンス鍵KDCによる  
暗号文

ROM型の記録媒体のディTSAMの記憶データ(登録及び購入処理後)

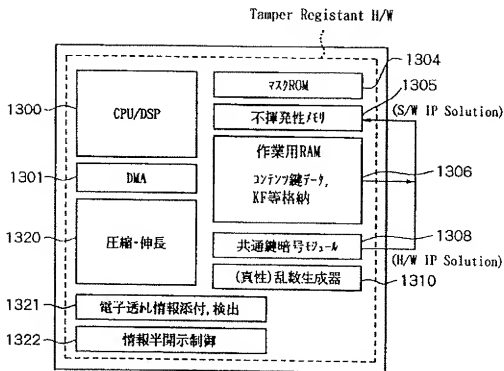
【図77】

ディジタルID	
記録用鍵KSTR(ディジタル鍵KMD)	
User ID	
パスワード	
個人嗜好情報	
個人決済情報(クレジットカード番号)	
電子マネー	
第3信頼機関(EMV+ピスセン)の公開鍵	
ルートCAの公開鍵	
ディジタル公開鍵証明書(X.509)	
ディジタル公開鍵・秘密鍵	
Revocation List(更新値)	
権利処理(利益配分)用データ	
利益分配に関与したエンティティのID	
ディジタル ・ディジタル種別情報 ・ROM/RAM	
キーファイルKFの物理アドレス情報 (レジスタ空間)	検証値
検証値(MAC)	
コンテンツ番号-#1のKF/KF <sub>1</sub>	
コンテンツ番号-#2のKF/KF <sub>1</sub>	
コンテンツ番号-#3のKF/KF <sub>1</sub>	
コンテンツ番号-#4のKF/KF <sub>1</sub>	
コンテンツ番号-#5のKF/KF <sub>1</sub>	
	検証値 (MAC)
コンテンツ番号-#nのKF/KF <sub>1</sub>	
検証値(MAC)	

記録用鍵KSTRによる  
暗号文

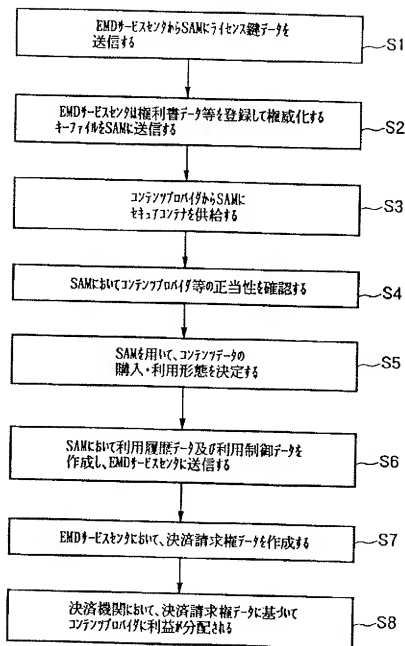
RAMの記録媒体のディジタルIDの記憶データ(登録及び購入処理後)

【図78】

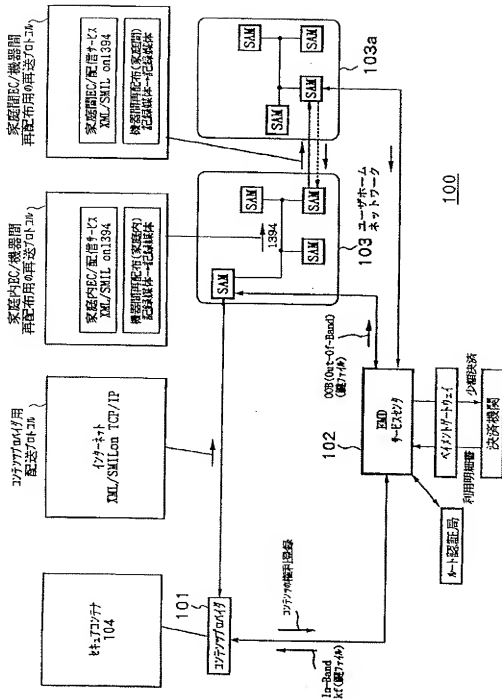


AVI圧縮・伸長用SAM163

【図80】



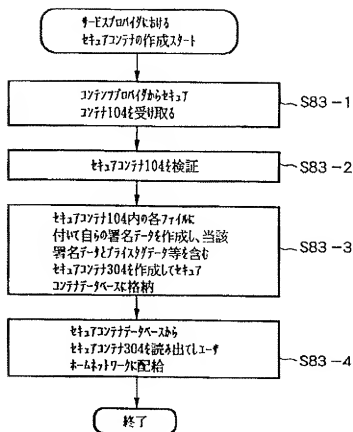
【圖 8 1】



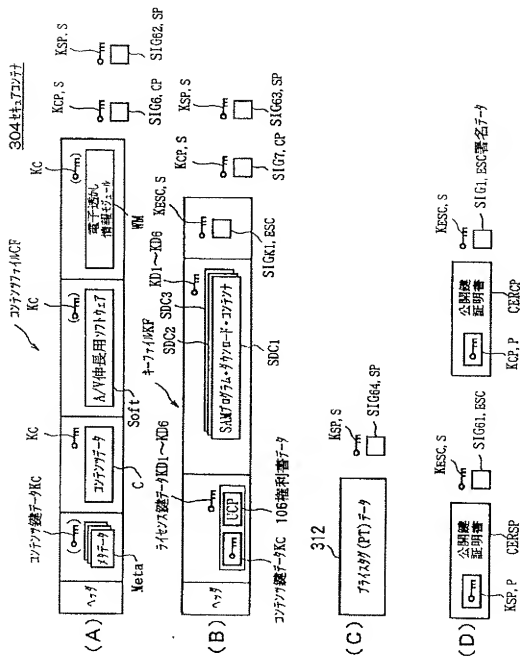


[illegible]

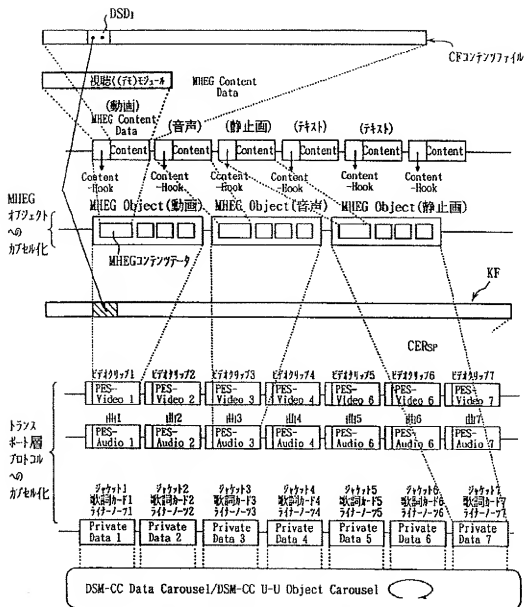
【図 8 3】



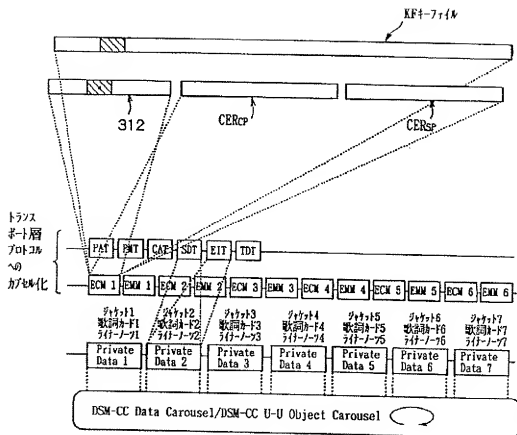
【図84】



【図 85】



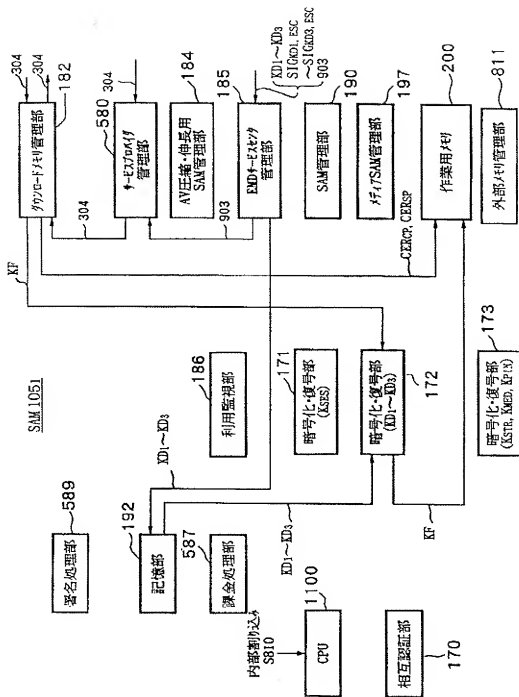
【図86】





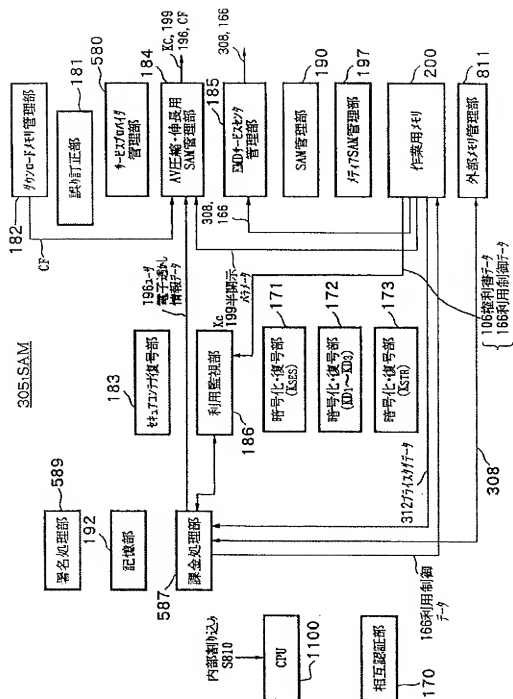


【圖 90】

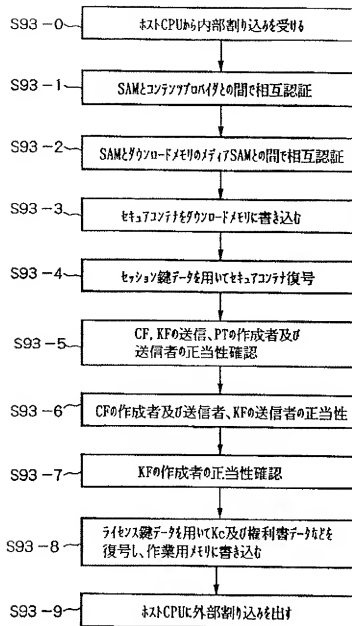




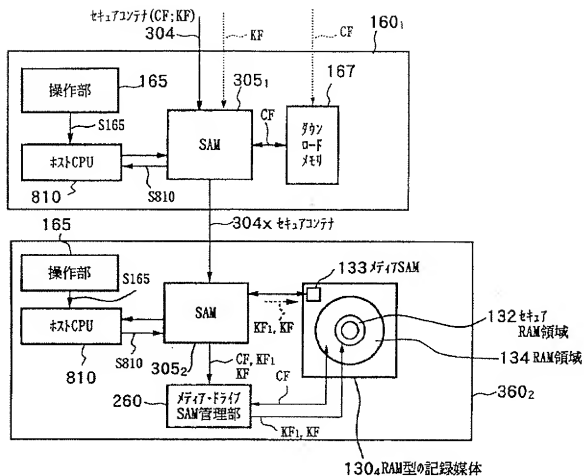
[図 9 2]



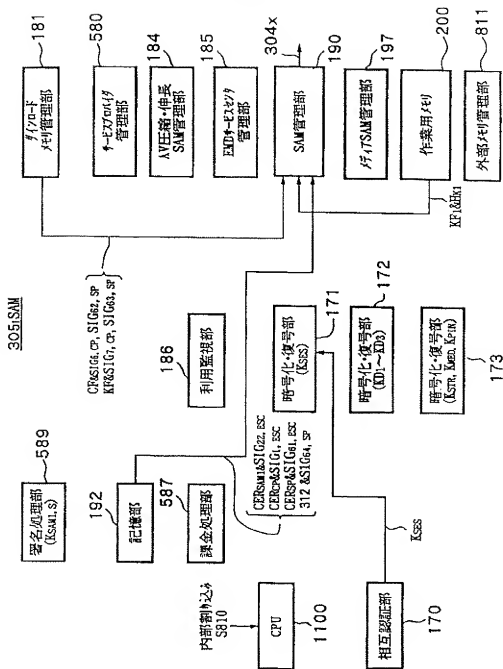
【図93】

セキアコンテの入力処理 (SAM)

【图 9-4】

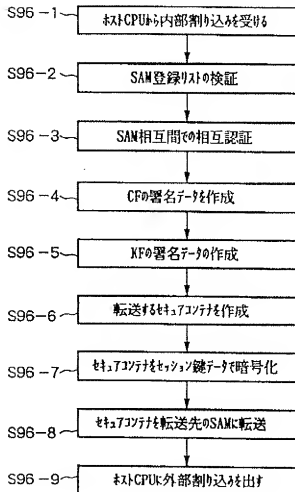


[図 9 5]

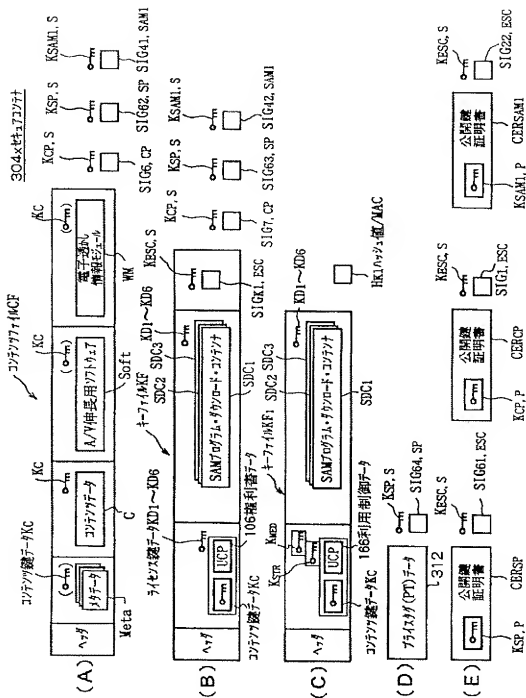


【図96】

一の機器の利用制御データを使用して他の機器を  
再購入を行う場合の転送元のSAMの処理 (SAM3051)



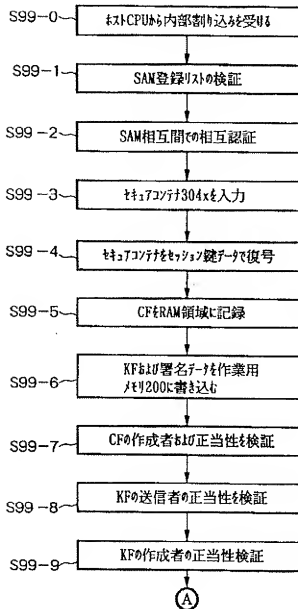
【図 97】





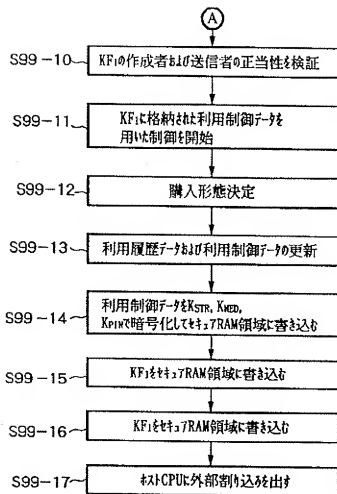
【図99】

一の機器の利用制御データを使用して他の機器で  
再購入を行う場合の転送先のSAMの処理 (SAM3052)



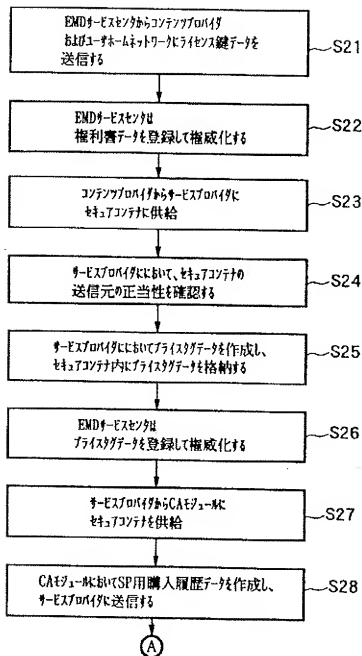


【図100】

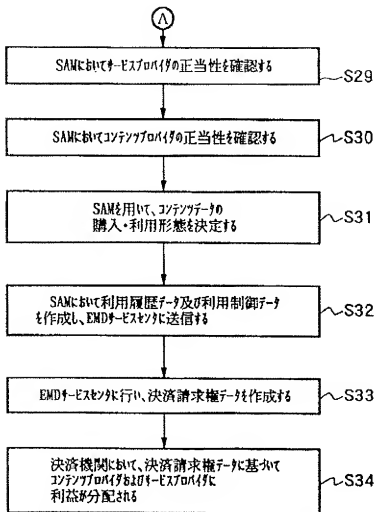




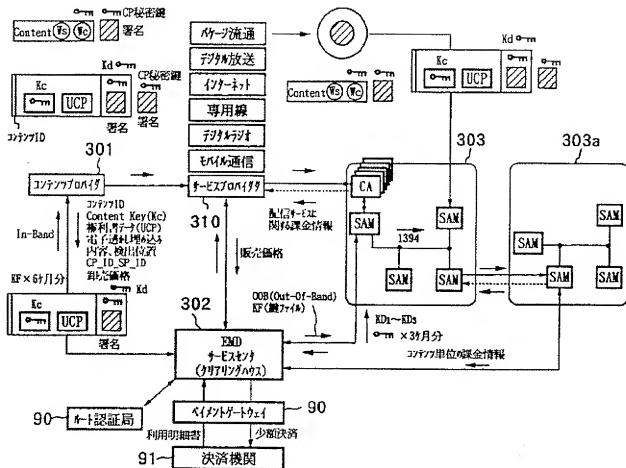
【図102】



【図103】

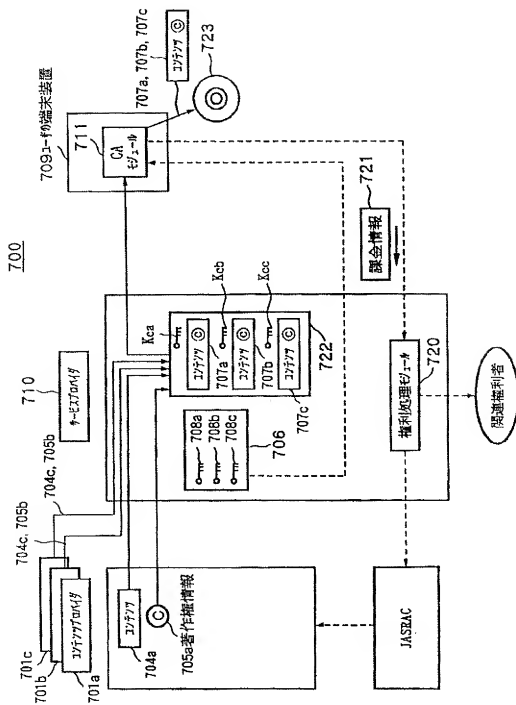


【図104】





【図106】



フロントページの続き

Fターム(参考) 5B085 AE13 AE23 AE29  
5B089 GA19 JA33 JB05 KA17 KB13  
KC09 KC57 KC58 KH30  
5J104 AA01 AA09 AA16 AA46 EA01  
EA06 EA17 LA06 NA02 NA42  
PA07 PA10  
9A001 CZ02 EE03 JJ19 KK43 KK60  
KK62